Secure refinements of communication channels

Vincent Cheval, Véronique Cortier, Eric Le Morvan

Secure refinements of communication channels

Vincent Cheval[1,3], Véronique Cortier[2], and Eric le Morvan[2]

1 **School of Computing, University of Kent, UK**
2 **LORIA, CNRS, France**
3 **LORIA, INRIA, France**

Abstract

It is a common practice to design a protocol (say Q) assuming some secure channels. Then the secure channels are implemented using any standard protocol, e.g. TLS. In this paper, we study when such a practice is indeed secure.

We provide a characterization of both confidential and authenticated channels. As an application, we study several protocols of the literature including TLS and BAC protocols. Thanks to our result, we can consider a larger number of sessions when analyzing complex protocols resulting from explicit implementation of the secure channels of some more abstract protocol Q.

1 Introduction

When designing a protocol, it is common to assume a secure, confidential, or authentic channel. Authentic channels may be read but not written in. Symmetrically, confidential channels may be written in but not read. Secure channels are both authentic and confidential. For example, payment protocols like 3D-secure are supposed to be run over a secure channel such as TLS. Similarly, many services such as public key registration assume an authenticated channel. How to implement these secure channels is left unspecified and, intuitively, the security of a payment protocol should not depend on the particular choice of implementation of its secure channels. A typical example of a popular and generic realization of a secure channel is TLS. For authentication, one usually relies on a password-based authentication or on previously established keys (used e.g. for signature or MACs). Is it safe to use these protocols in any context? What is a secure or authenticated channel? This paper aims at characterizing channels that have security properties. For example, assume Q is a secure protocol (e.g. a payment protocol) that requires a secure channel. Which properties should a protocol P achieve in order to securely realize the secure channels of Q? These properties should of course be independent of Q since P and Q are typically designed in totally independent contexts. In the remaining of this introduction, Q will refer to the "main" protocol while P will refer to a protocol realizing secure channels (for several notions of security).

Our contributions. Our first contribution is a characterization of both secure, confidential, and authenticated channels. We actually characterize what it means for a channel to be readable or not, and writable or not. Then the realization of a secure channel typically proceeds in two phases. First, some values are established by the protocol P, for example short-term symmetric keys or MAC keys. Quite unsurprisingly, we show that these values need to be secret and appropriately shared. Then the messages of Q are transported or *encapsulated* using the values established by P. For example, the messages of Q may be encrypted with a key established by P. We provide a characterization of secure encapsulations both for secure, confidential, and authentic channels. A key feature of our characterization is that it is independent of P and Q, which allows for a modular analysis. We show that standard encapsulations (e.g. typical use of encryption, signatures, or MACs) enjoy the requested properties.

Our second and main contribution is to show how to securely compose protocols. Intuitively, our main result guarantees that whenever P is a secure key exchange protocol and $\mathcal{E}$ is a secure

encapsulation then $P \cdot^{\mathcal{E}} Q$ is as secure as Q where $P \cdot^{\mathcal{E}} Q$ denotes the protocol obtained from Q by implementing its secure channels using P and $\mathcal{E}$.

The interest of our result is twofolds. First, it provides foundational grounds to a common practice where protocols are typically designed and studied independently and then combined. We show that such a practice is actually secure under reasonably light assumptions: primitives shared between P, $\mathcal{E}$, and Q should be tagged as proposed in [4]. Tagging is a standard practice that avoids message confusion. Second, our result provides a technique for analyzing a complex protocol: it is sufficient to analyse its components to deduce security of the whole protocol. To express and prove our result, we have developed a framework, an extension of the applied-pi calculus [2], that allows to easily talk about protocols roles and sessions, a missing aspect in the applied-pi calculus.

To illustrate our approach, we show that TLS is a secure implementation of secure channels. Similarly we show that the BAC protocol [1] is also a secure implementation of a secure channel and may be safely used with the Passive Authentication (PA) protocol as prescribed for the biometric passport [1]. Using the CL-Atse tool [18], we analyse several combined protocols. Thanks to our combination result, it is possible to analyse protocols in isolation instead of their combination, which allows to consider a larger number of sessions.

Related work. One seminal work on composition is the one of Guttman and Thayer [13]. They show that two protocols can be composed without one damaging the security of the other as soon as they are "independent". However, this independence notion needs to be checked for any protocol execution and cannot be statically checked at the protocol specification level. Later, Guttman [11] provides a criterion on the specification of P and Q such that P can be safely composed with Q. Intuitively, Q should not break some invariant satisfied by P and conversely. While the work of [11] focuses on authentication and secrecy properties, [12] more generally devises a framework for defining protocol goals and designing, step by step, protocols that fulfill them. In [10], the strand space model is used in a modular way, to analyse protocols components by components. The disjunction criteria cannot be checked statically. All these approaches provide a framework that allows to reason modularly when analysing the combination of two protocols P and Q, typically expressing invariants satisfied by P that are shown sufficient to prove security of Q. This simplifies the proof of P combined with Q but requires the knowledge of both protocols. Compared to our work, we propose a criteria for a protocol P to securely implement a secure channel, independently of the protocol Q that will use it (provided primitives are tagged).

Under tagging assumptions similar to ours, it was already shown that P and Q can be safely run in parallel even if they share long-term keys [7]. In passing, we generalize this result to the case where long-term keys may be used as payload. [6] explains when two protocols may be used sequentially, with Q using data established by P. The main difference with our work is that messages may not be transformed when composing protocols. Therefore, [7, 6] cannot be used to (securely) implement abstract channels. Note also that [6] may not consider compromised sessions, that is sessions between honest and dishonest agents. The problem we address here is referred to as *sequential composition* in [16], where the messages of Q are used as payloads in the composed protocol $P \cdot^{\mathcal{E}} Q$. [16] provides a nice exposition of the generic problem of a protocol Q using a protocol P as subprotocol and lists sufficient (semantical) conditions for combining two protocols. These conditions require again the knowledge of both P and Q.

Datta et al. (e.g. [8]) have also studied secure protocol composition in a broader sense: protocols can be composed in parallel, sequentially or protocols may use other protocols as components. However, they do not provide any syntactic conditions for a protocol P to be safely executed in parallel with other protocols. For any protocol P' that might be executed in parallel, they have to prove that the two protocols P and P' satisfy each other invariants. Their approach is thus rather designed for component based design of protocols.

2 Model

Our model is inspired from the applied-pi calculus [2], extended to an explicit notion of roles.

2.1 Messages

Messages are modeled using a typed term algebra. We assume an infinite set of names $\mathcal{N} = \mathcal{N}_D \uplus \mathcal{N}_H$ of *base type* and a set Ch of names of *channel type*. The set $\mathcal{N}_H$ (resp. $\mathcal{N}_D$) represents the names accessible by honest (resp. dishonest) agents. We also a consider an infinite set of variables $\mathcal{X}$ and a finite signature $\mathcal{F}$ of function symbols operating and returning terms of *base type*. More precisely, we consider $\mathcal{F} = \mathcal{F}_c \uplus \mathcal{F}_{cst} \uplus \mathcal{F}_{key}$ where $\mathcal{F}_{cst}$ contains only constants, all functions in $\mathcal{F}_{key}$ are unary, and $\mathcal{F}_c = \{\langle\,\rangle/2, \mathsf{f}_1/n_1, \ldots, \mathsf{f}_k/n_k\}$ contains the binary function symbol $\langle\,\rangle$ used to denote concatenation and other function symbols f_i of arity n_i. Terms are defined as names, variables and function symbols applied to other terms. The set of terms built from $N \subseteq \mathcal{N} \cup Ch$, $X \subseteq \mathcal{X}$ and by applying the function symbols in $F \subseteq \mathcal{F}$ is denoted by $\mathcal{T}(F, N \cup X)$. We denote by $st(t)$ the set of subterms of t. We denote by $vars(t)$ (resp. $names(t)$) the set of variables (resp. names) in t. When $vars(t) = \emptyset$, we say that t is *ground*. To represent events that may occur during a protocol execution, we assume an infinite signature $\mathcal{E}v$ distinct from $\mathcal{F}$. We say that a term $e(t_1, \ldots, t_n)$ with $e \in \mathcal{E}v$ and $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathcal{X})$ is an event.

▶ **Example 1.** A standard signature to represent encryption and signature is $\mathcal{F}_{std}$, the signature built from a finite set of constants, functions $\mathcal{F}_{cstd} = \{\mathsf{senc}/2, \mathsf{aenc}/2, \mathsf{sign}/2, \mathsf{h}/1, \langle\rangle/2\}$ and $\mathcal{F}_{kstd} = \{\mathsf{pk}/1, \mathsf{vk}/1\}$. The function symbol senc (resp. aenc) represents the symmetric (resp. asymmetric) encryption. We denote by $\mathsf{pk}(s)$ the public key associated s. The function symbol sign represents the digital signature where $\mathsf{vk}(s)$ is the verification associated to s. We write $\langle u, v\rangle$ as syntactic sugar for $\langle\rangle(u, v)$.

We model the algebraic properties of the cryptographic primitives by a set of inference rules $\mathcal{I}$ composed of composition and decomposition rule described as follows:

$$\frac{x_1 \quad \ldots \quad x_k}{\mathsf{f}(x_1, \ldots, x_k)}\ \text{f-comp} \qquad \frac{\langle x_1, x_2\rangle}{x_1} \qquad \frac{\langle x_1, x_2\rangle}{x_2} \qquad \frac{\mathsf{f}(x, u_1, \ldots, u_n) \quad v_1 \quad \ldots \quad v_m}{x}\ \text{f-decomp}$$

where for all $j \in \{1, \ldots, n\}$, for all $k \in \{1, \ldots, m\}$, $u_j, v_k \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ and $vars(v_1, \ldots, v_k) \subseteq \{u_1, \ldots, u_n, x\}$. For each $\mathsf{f} \in \mathcal{F}$, the set $\mathcal{I}$ contains a unique f-comp rule and there is no f-decomp rule when $\mathsf{f} \in \mathcal{F}_{key}$. Given a set or sequence of terms S and a term t, the deducibility relation is inductively defined as follows. The term t is deducible from S, denoted $S \vdash t$, when $t \in S \cup \mathcal{F}_{cst} \cup \mathcal{N}_D$ or there exists a substitution σ and an inference rule in $\mathcal{I}$ with premisses $u_1, \ldots, u_n$ and conclusion u such that $t = u\sigma$ and for all $i \in \{1, \ldots, n\}$, $S \vdash u_i\sigma$.

▶ **Example 2.** Continuing Example 1, we define the set $\mathcal{I}_{std}$ of decomposition rules as follows.

$$\frac{\mathsf{senc}(x, y) \quad y}{x} \qquad \frac{\mathsf{aenc}(x, \mathsf{pk}(y)) \quad y}{x} \qquad \frac{\mathsf{sign}(x, y) \quad \mathsf{vk}(y)}{x} \qquad \frac{\langle x, y\rangle}{x} \qquad \frac{\langle x, y\rangle}{y}$$

We have that $\mathsf{senc}(\langle a, c\rangle, k), k \vdash a$ but $\mathsf{aenc}(\langle a, c\rangle, \mathsf{pk}(k)), \mathsf{pk}(k) \nvdash a$.

2.2 Agents

In standard process algebra (*e.g.* [2]), the notion of agents is usually implicit. Typically, a process that models the behavior of the different honest agents is a single process where all agents are implicitly represented. However, to model protocol composition, we need to explain how to compose each role and thus we need to talk about each agent separately. Therefore, we explicit the presence of agents

in our model. Interestingly, our model may also be used to specify semi-honest agents which may directly communicate with the attacker during the protocol execution, still hiding some secrets from him. We consider an infinite set of agents $\mathcal{A}gt = \{A, B, \ldots\} = \mathcal{A}gt_H \uplus \mathcal{A}gt_D$ where $\mathcal{A}gt_H$ and $\mathcal{A}gt_D$ represent respectively honest and dishonest agents. Each agent possesses private data such as keys. Therefore, we consider $\mathcal{N}_{\mathcal{A}gt}$ a subset of $\mathcal{N}$ as an infinite partition $\mathcal{N}_{\mathcal{A}gt} = \biguplus_{A \in \mathcal{A}gt} \mathcal{N}_A$ where $\mathcal{N}_A$ intuitively are the names accessible by the agent A. By convention, $k[A]$ denotes a name in $\mathcal{N}_A$.

2.3 Protocols

In the spirit of [2], we model protocols through a process algebra. We represent explicitly confidential, secure, and authenticated channels. Formally, we partition the set of channels into three infinite sets $Ch = Ch_a \uplus Ch_c \uplus Ch_s \uplus Ch_p$ where Ch_a, Ch_c, Ch_s, Ch_p respectively represent the sets of authenticated, confidential, secure and public channels. The syntax of our calculus is as follows:

Roles of agent A

$$R_A, R'_A := \quad 0 \mid \mathsf{out}_A(c,u).R_A \mid \mathsf{in}_A(c,v).R_A \mid \mathsf{new}\ k.R_A \mid \mathsf{event}_A(ev).R_A$$

Channel and agent declarations

$$C, C' := \quad R_A \mid \mathsf{new}_{ta}\ c.C \mid C \mid C'$$

Processes

$$P, Q := \quad C \mid P \mid Q \mid !P \mid \mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub}, \mathcal{K}_{prv}).P$$

where $c \in Ch$, $A \in \mathcal{A}gt$, ta is the tuple of agents in C such that c occurs in their role, k is name, u and v are terms, ev is an event, $\mathcal{K}_{pub}$ and $\mathcal{K}_{prv}$ are sets of ground terms with $names(\mathcal{K}_{pub}) \subseteq \mathcal{N}_A$, $names(\mathcal{K}_{prv}) \subseteq \mathcal{N}_{\mathcal{A}gt}$ and $\mathcal{A} \subseteq \mathcal{A}gt$.

The behavior of an agent A is described in a *role* R_A that consists of a sequence of inputs, outputs, creations of names and emissions of events. The role $\mathsf{out}_A(c,u).R_A$ outputs the term u on the channel c and then behaves like R_A. The role $\mathsf{in}_A(c,v).R_A$ inputs a message from channel c and expects it to be an instance of v. The role $\mathsf{new}\ k.R_A$ generates a fresh name k. Processes express how the roles of different agents are combined. The process $\mathsf{new}_{ta}\ c$ allocates an abstract channel to the agents in ta. The process $P \mid Q$ expresses the parallel execution of P and Q. The process $!P$ represents the replication of P. The process $\mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub}, \mathcal{K}_{prv}).P$ selects a new agent A amongst $\mathcal{A}$. The set $\mathcal{K}_{pub}$ typically indicates the public keys of A while $\mathcal{K}_{prv}$ contains the (secret) long term keys known by A. The variables in a role are uniquely bound by the first input in which they appear. The channels are bound by the operators new . The agents in a process are also bound by agent creation. In a protocol, we assume that a name or variable is syntactically bound only once. A variable (resp. agent, channel) that is not bound in P is free. We denote by $fa(P)$, $ba(P)$, $fv(P)$, $bv(P)$, $fn(P)$ and $bn(P)$ the sets of free and bound agents, variables and names in P respectively. We say that P is closed when $fv(P) = \emptyset$. Given a process P and an agent A, we denote by $names_A(P)$ and $ch_A(P)$ the sets of names, channels that occur in the roles of A in P.

A role is executable if it only outputs terms that may be deduced from its inputs, the generated values (nonces and keys), and the long-term keys used in the role.

▶ **Definition 3.** Let $R_A = r_1 \ldots . r_n$ be a role of an agent A. We say that R_A is *executable* when for all $i \in \{1, \ldots, n\}$, if $r_i = \mathsf{out}_A(c,u)$ then $names(r_1, \ldots, r_i) \cup S \vdash u$ where $S = \{v \mid j < i \wedge (r_j = \mathsf{in}_A(d,v) \vee r_j = \mathsf{new}\ v)\}$. A process P is executable when all the roles in P are executable.

The state of a protocol during its execution is represented by a *configuration* (P, Φ, μ, θ) where P is a closed process, Φ is a sequence of ground terms representing the knowledge of the attacker, μ is a mapping from channels to sets of terms representing the messages sent over non-public channels and θ is a mapping from triplets of channel, agent, tuple of agents to sets of channels. The semantics

$(P \mid \mathsf{out}_A(c,u).R_A, \Phi, \mu, \theta) \to (P \mid R_A, \Phi', \mu', \theta)$ where $\Phi' = \Phi$ if $c \in Ch_c \cup Ch_s$ else $\Phi' = \Phi \cdot [u]$ and $\mu' = \mathsf{rect}(c,u,\mu)$ if $c \notin Ch_p$ else $\mu' = \mu$ — OUT

$(P \mid \mathsf{in}_A(c,v).R_A, \Phi, \mu, \theta) \to (P \mid R_A\sigma, \Phi, \mu, \theta)$ if there exists σ such that $dom(\sigma) = vars(v)$ and either $v\sigma \in c\mu$ or else $c \in Ch_p \cup Ch_c$ and $\Phi \vdash v\sigma$ — IN

$(P \mid \mathsf{new}\ k.R_A, \Phi, \mu, \theta) \to (P \mid R_A\{^{k'}/_k\}, \Phi, \mu, \theta)$ with k' fresh in $\mathcal{N}_H$ if $A \in \mathcal{A}gt_H$ else $k' \in \mathcal{N}_D$ — NEW-K

$(P \mid \mathsf{new}_{ta}\ c.C[R_{A_1}, \ldots, R_{A_n}], \Phi, \mu, \theta) \to (P \mid [R'_{A_1}, \ldots, R'_{A_n}], \Phi, \mu, \theta')$ — NEW-C
$\forall i, R'_{A_i} = R_{A_i}$ if $c \notin ch(R_{A_i})$ else $R'_{A_i} = R_{A_i}\{^{c_{A_i}}/_c\}$ with $c_{A_i} \in Ch_p$ if $ta \cap \mathcal{A}gt_D \neq \emptyset$ else $c_{A_i} \in S \cup \bigcup_{B \in ta} \theta(c,B,ta) \setminus \theta(c,A_i,ta)$ and $S \subseteq Ch_a$ fresh (resp. Ch_c, Ch_s) if $c \in Ch_a$ (resp. Ch_c, Ch_s). Moreover, $\theta = \theta'$ if $ta \cap \mathcal{A}gt_D \neq \emptyset$ else $\theta' = \mathsf{recc}(\{(c_A, A)\}_{A \in ta}, ta, c, \theta)$.

$(P \mid !Q, \Phi, \mu, \theta) \to (P \mid !Q \mid Q\rho, \Phi, \mu, \theta)$ with ρ a fresh renaming of $vars(Q)$ — REPL

$(P \mid \mathsf{event}_A(ev).R, \Phi, \mu, \theta) \xrightarrow{ev} (P \mid R, \Phi, \mu, \theta)$ — EVENT

$(P \mid \mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub}, \mathcal{K}_{prv}).Q, \Phi, \mu, \theta) \to (P \mid Q\sigma, \Phi \cdot S, \mu, \theta)$ — AGENT
with $\sigma = \{^{A'}/_A\}$, $A' \notin fa(Q)$, $S = \mathcal{K}_{pub}\sigma$ if $A' \in \mathcal{A} \cap \mathcal{A}gt_H$ else $S = \mathcal{K}_{pub}\sigma \cdot \mathcal{K}_{prv}\sigma$

Figure 1 Semantics of configuration

is given in Figure 1. The rule OUT indicates that the attacker obtains messages on public or authenticated channels. In this rule, $\mathsf{rect}(c,t,\mu)$ is the mapping μ' where t was recorded as being sent over c. Formally, $\mu'(c') = \mu(c')$ for any $c' \neq c$ and $\mu'(c) = \mu(c) \cup \{t\}$. With rule IN the attacker can inject on c any message that he can deduce from his knowledge when c is a public or confidential channel. He can also relay any message that was previously sent on c. The rule NEW-K generates a fresh name of $\mathcal{N}_H$ or $\mathcal{N}_D$ depending on whether the agent A is honest or not. The rule NEW-C allocates to the role of an agent a channel possibly fresh or that has already been used by other roles in different sessions. In this rule, $\mathsf{recc}(S, ta, c, \theta)$ is the mapping θ in which we record the channels allocated to the agents. Formally, $\theta'(c', A', ta') = \theta(c', A', ta')$ for any $A' \notin ta'$ or $(c', ta') \neq (c, ta)$, and $\theta'(c, A, ta) = \theta(c, A, ta) \cup \{d\}$ for any $(d, A) \in S$. The rule AGENT selects an agent from $\mathcal{A}$ and adds $\mathcal{K}_{pub}$ to the knowledge of the attacker. Additionally, if the agent is dishonest, the rules adds $\mathcal{K}_{prv}$. When $(P, \Phi, \mu, \theta) \xrightarrow{e_1} \ldots \xrightarrow{e_n} (P', \Phi', \mu', \theta')$, we write $(P, \Phi, \mu, \theta) \xRightarrow{e_1 \cdot \ldots \cdot e_n} (P', \Phi', \mu', \theta')$.

▶ **Example 4.** An electronic passport is a paper passport containing a RFID chip that stores most of the information printed on the passport. The protocols used to access these private data are specified in the International Civil Aviation Organization standard [1]. Before exchanging any private data, an electronic passport and a reader must establish session keys through a key-exchange protocol, called Basic Access Control (BAC), that prevents eavesdropping on further communication. The BAC protocol relies on two keys ke and km that are printed on the passport and thus can be obtained by the reader through optical scanning. We described below the BAC protocol, between a passport (P) and a reader (R). We assume encrypted messages to be tagged with a. The use of tagging will be explained later on.

$$\mathsf{R} \to \mathsf{P} : \mathsf{challenge}$$
$$\mathsf{P} \to \mathsf{R} : n_\mathsf{P}$$
$$\mathsf{R} \to \mathsf{P} : \langle \mathsf{senc}(\langle \mathsf{a}, n_\mathsf{R}, n_\mathsf{P}, k_\mathsf{R} \rangle, ke), \mathsf{mac}(\langle \mathsf{a}, \mathsf{senc}(\langle \mathsf{a}, n_\mathsf{R}, n_\mathsf{P}, k_\mathsf{R} \rangle, ke) \rangle, km) \rangle$$
$$\mathsf{P} \to \mathsf{R} : \langle \mathsf{senc}(\langle \mathsf{a}, n_\mathsf{P}, n_\mathsf{R}, k_\mathsf{P} \rangle, ke), \mathsf{mac}(\langle \mathsf{a}, \mathsf{senc}(\langle \mathsf{a}, n_\mathsf{P}, n_\mathsf{R}, k_\mathsf{P} \rangle, ke) \rangle, km) \rangle$$

After receiving a challenge command from the reader, the passport generates a fresh name n_P that

will be used to verify the authenticity of the messages he will receive later on. Upon receiving n_{P}, the reader generates two nonces $n_{\mathsf{R}}, k_{\mathsf{R}}$ and sends back to the passport all three nonces encrypted with the key k_e and a mac with the key k_m. The nonce n_{R} has also an authenticity purpose whereas k_{R} will be the reader's contribution to the session keys. The passport then checks the mac using k_m and the cipher by decrypting it using k_e and verifying the presence of n_{P} in the plain text. If all verifications succeed, the passport generates a nonce k_{P}, the passport's contribution to the session keys, and sends it to the reader. At the end of the protocol, both reader and passport know k_{R} and k_{P} that they use to generate two session keys $\mathsf{f}_1(k_{\mathsf{R}}, k_{\mathsf{P}})$ and $\mathsf{f}_2(k_{\mathsf{R}}, k_{\mathsf{P}})$. In our syntax, the roles of the reader (R_{R}) and of the passport (R_{P}) can be expressed as follows.

$$\begin{aligned} R_{\mathsf{P}} = \;& \mathsf{in}_{\mathsf{P}}(c, \mathsf{challenge}).\mathsf{new}\ n_{\mathsf{P}}.\mathsf{out}_{\mathsf{P}}(c, n_{\mathsf{P}}).\mathsf{in}_{\mathsf{P}}(c, \langle M, \mathsf{mac}(\langle \mathsf{a}, M\rangle, km[\mathsf{P}]\rangle)). \\ & \mathsf{new}\ k_{\mathsf{P}}.\mathsf{out}_{\mathsf{P}}(c, \langle N, \mathsf{mac}(\langle \mathsf{a}, N\rangle, km[\mathsf{P}]\rangle)).0 \end{aligned}$$

$$\begin{aligned} R_{\mathsf{R}} = \;& \mathsf{out}_{\mathsf{R}}(c, \mathsf{challenge}).\mathsf{in}_{\mathsf{R}}(c, z).\mathsf{new}\ k_{\mathsf{R}}.\mathsf{new}\ n_{\mathsf{R}}.\mathsf{out}_{\mathsf{R}}(c, \langle U, \mathsf{mac}(\langle \mathsf{a}, U\rangle, km[\mathsf{P}])). \\ & \mathsf{in}_{\mathsf{R}}(c, \langle V, \mathsf{mac}(\langle \mathsf{a}, V\rangle, km[\mathsf{P}]\rangle)).0 \end{aligned}$$

with $c \in Ch_p$, $M = \mathsf{senc}(\langle \mathsf{a}, x, n_{\mathsf{P}}, y\rangle, ke[\mathsf{P}])$, $N = \mathsf{senc}(\langle \mathsf{a}, n_{\mathsf{P}}, x, k_{\mathsf{P}}\rangle, ke[\mathsf{P}])$, $U = \mathsf{senc}(\langle \mathsf{a}, n_{\mathsf{R}}, z, k_{\mathsf{R}}\rangle, ke[\mathsf{P}])$ and $V = \mathsf{senc}(\langle \mathsf{a}, z, n_{\mathsf{R}}, w\rangle, ke[\mathsf{P}])$. An honest reader communicating with unbounded number of passports, possibly dishonest, can be modeled in our calculus as the process:

$$BAC = \; \mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}]\}).(R_{\mathsf{P}} \mid R_{\mathsf{R}})$$

where $\mathcal{P}$ is an infinite set of agents containing honest and dishonest agents and $\mathsf{R} \notin \mathcal{P}$. The following trace would correspond to the execution of a session with a dishonest passport I and a session of an honest one A both in $\mathcal{P}$.

$$\begin{aligned} (BAC, \emptyset, \emptyset, \emptyset) &\to^* (BAC \mid \mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}]\}).(R_{\mathsf{P}} \mid R_{\mathsf{R}}), \emptyset, \emptyset, \emptyset) \\ &\to (BAC \mid R_{\mathsf{P}}\sigma_A \mid R_{\mathsf{R}}\sigma_A, \emptyset, \emptyset, \emptyset) \\ &\to^* (BAC \mid R_{\mathsf{P}}\sigma_A \mid R_{\mathsf{R}}\sigma_A \mid R_{\mathsf{P}}\sigma_I \mid R_{\mathsf{R}}\sigma_I, [ke[\mathsf{I}], km[\mathsf{I}]], \emptyset, \emptyset) \\ &\to (BAC \mid R_{\mathsf{P}}\sigma_A \mid R_{\mathsf{R}}\sigma_A \mid R_{\mathsf{P}}\sigma_I \mid Q, [ke[\mathsf{I}], km[\mathsf{I}], \mathsf{challenge}], \emptyset, \emptyset) \\ &\to^* \ldots \end{aligned}$$

where $\mathsf{P}\sigma_A = \mathsf{A}$, $\mathsf{P}\sigma_I = \mathsf{I}$ and σ_A, σ_I also are fresh renaming of bound variables and names and $R_R\sigma_I = \mathsf{out}_{\mathsf{I}}(c, \mathsf{challenge}).Q$. By convention the empty mapping $\mu = \emptyset$ (resp. $\theta = \emptyset$) denotes the mapping that maps any argument to the emptyset: $\mu(c) = \emptyset$ (resp. $\theta(c, A, ta) = \emptyset$) for any c, A, ta.

3 Composition

In the previous section, we have defined an abstract notion of confidential, secure, and authenticated channels. In practice, such channels are realized through cryptographic means. Agents first execute some key establishment protocol in order to generate secret session keys. Then they *encapsulate* the messages supposedly sent over a channel using these session keys. A standard case for secure channels consists in using session keys to encrypt subsequent messages. How to encrypt the message is defined by the *encapsulation*. In Section 3.1, we provide a generic definition of encapsulations and identify properties needed for encapsulations to allow for authentication, confidential, and secure channels. We continue in Section 3.2 by characterizing the composition of a key establishment protocol with a process using abstract channels.

3.1 Encapsulation

For our composition result, we *tag* encapsulations and processes. These tags are used to distinguish the parts of a message that correspond to encapsulations from the ones coming from processes. Formally, a tag is a constant from $\mathcal{F}_{cst}$, hence known to the attacker. Given a set $\mathsf{Tag} \subseteq \mathcal{F}_{cst}$, we say that a term t is a Tag-term when for all $t' \in st(t)$, if $t' = \mathsf{f}(t_1, \ldots, t_n)$ for some $\mathsf{f} \in \mathcal{F}_c \backslash \{\langle\ \rangle\}$ and some

terms $t_1, \ldots, t_n$ then $t_1 = \langle \mathsf{a}, u \rangle$ for some term u and $\mathsf{a} \in \mathsf{Tag}$.

▶ **Definition 5.** A Tag-encapsulation is a pair $(\mathcal{E}, \mathsf{F})$ where $\mathcal{E}$ is a Tag-term of $\mathcal{T}(\mathcal{F}, \mathcal{X})$ and $\mathsf{F} \subseteq \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ such that $vars(\mathcal{E}) = \{x, x_1, \ldots, x_n\}$, $\{\mathcal{E}, x_1, \ldots, x_n\} \vdash x$ and for all $t \in st(\mathcal{E})$,

- if $t = \mathsf{f}(v)$ with $\mathsf{f} \in \mathcal{F}_{key}$ then $v \in \{x_1, \ldots, x_n\} \cup \mathcal{F}_{cst}$
- if $t = \mathsf{f}(w, t_1, \ldots, t_n)$ and there exists a f-decomposition rule with $\mathsf{f}(x, u_1, \ldots, u_n), v_1, \ldots, v_m$ as premises then for all $j \in \{1, \ldots, m\}$, for all $i \in \{1, \ldots, n\}$, $v_j = \mathsf{g}(y)$ and $y \in vars(u_i)$ implies $t_i \in \{x_1, \ldots, x_n\} \cup \mathcal{F}_{cst}$. Intuitively, if a f-decomposition rule may be applied to a subterm of an encapsulation using a non atomic key $\mathsf{g}(t_i)$ then t_i must be a variable or a constant.

We denote x by $\mathsf{t}_\mathcal{E}$ and $(x_1, \ldots, x_n)$ by $\mathsf{X}_\mathcal{E}$. Given two encapsulations $(\mathcal{E}, \mathsf{F})$ and $(\mathcal{E}', \mathsf{F}')$, we write $\mathcal{E} \sim \mathcal{E}'$ when there exists a renaming ρ such that $\mathcal{E}\rho = \mathcal{E}'$, $\mathsf{F}\rho = \mathsf{F}'$, $\mathsf{t}_\mathcal{E}\rho = \mathsf{t}_{\mathcal{E}'}$ and $\mathsf{X}_\mathcal{E}\rho = \mathsf{X}_{\mathcal{E}'}$. We denote by $\mathcal{E}(t, t_1, \ldots, t_n)$ the term obtained from $\mathcal{E}$ by substituting x by t and x_i by t_i.

In an encapsulation $(\mathcal{E}, \mathsf{F})$, the variable $\mathsf{t}_\mathcal{E}$ will be instantiated by the message sent on the channel implemented by the encapsulation whereas the variables in $\mathsf{X}_\mathcal{E}$ will be instantiated by the session keys. Note that $\{\mathcal{E}, x_1, \ldots, x_n\} \vdash x$ indicates that an encapsulated messages may always be retrieved using the session keys. The terms in F represent the public keys that can be used to deduce the term encapsulated or to generate an encapsulation with a new message without revealing the session keys.

▶ **Example 6.** In Example 4, we described how the session keys $\mathsf{f}_1(k_\mathsf{R}, k_\mathsf{P})$ and $\mathsf{f}_2(k_\mathsf{R}, k_\mathsf{P})$ are established in the BAC protocol. The ICAO standard states that in any other protocol executed after BAC, the messages exchanged should be of the form $\langle u, \mathsf{mac}(\langle \mathsf{b}, u \rangle, \mathsf{f}_1(k_\mathsf{R}, k_\mathsf{P})) \rangle$ with $u = \mathsf{senc}(\langle \mathsf{b}, M \rangle, \mathsf{f}_2(k_\mathsf{R}, k_\mathsf{P}))$ for some data M and tag b. This represents in fact the encapsulation of M with the session keys $\mathsf{f}_1(k_\mathsf{R}, k_\mathsf{P})$ and $\mathsf{f}_2(k_\mathsf{R}, k_\mathsf{P})$. In our formalism, the encapsulation is defined as $(\mathcal{E}_{\mathsf{BAC}}, \emptyset)$ where $\mathcal{E}_{\mathsf{BAC}} = \langle t, \mathsf{mac}(\langle \mathsf{b}, t \rangle, x_2) \rangle$ with $t = \mathsf{senc}(\langle \mathsf{b}, x \rangle, x_1)$, $\mathsf{t}_{\mathcal{E}_{\mathsf{BAC}}} = x$ and $\mathsf{X}_{\mathcal{E}_{\mathsf{BAC}}} = (x_1, x_2)$.

We use tags to distinguish the encapsulations from the messages actually sent over the network. However, a process can implement different types of channels using different encapsulations with the same tags. We need to ensure that the security of an encapsulation is not compromised when used with other encapsulations. Therefore, to state the different properties that encapsulations must satisfy, we consider a set of encapsulations and not only a unique one.

These conditions are easily met by standard encapsulations.

▶ **Definition 7.** Let $\mathcal{S}_e = \mathcal{S}_a \uplus \mathcal{S}_c \uplus \mathcal{S}_s$ be a set of Tag-encapsulations. We say that $\mathcal{S}_e$ allows authentic, confidential and secure channels if the following properties are satisfied: Let $(\mathcal{E}_1, \mathsf{F}_1), \ldots, (\mathcal{E}_n, \mathsf{F}_n) \in \mathcal{S}_e$. Assume that the variables in $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are disjoint. Let σ be a ground substitution such that $dom(\sigma) = vars(\mathcal{E}_1, \ldots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{Tag} \cap st(\sigma, \Phi) = \emptyset$. Let I be the set of $i \in \{1, \ldots, n\}$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$.

1. For all $i \in \{1, \ldots, n\}$, $\forall u \in \mathcal{T}(\mathcal{F}_{key}, \mathsf{X}_{\mathcal{E}_i}\sigma)$, if $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash u$ then $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k \in I} \vdash u$.
2. For all $i, i' \in \{1, \ldots, n\}$, $\forall u \in st(\mathcal{E}_i) \setminus \mathcal{X}$, $\forall v \in st(\mathcal{E}_{i'}) \setminus \mathcal{X}$, if u and v are unifiable and $\mathsf{root}(u) \neq \{\langle\,\rangle\}$ then $img(mgu(u, v)) \subset \mathcal{X}$.

Moreover, an encapulation is *authentic*, that is $(\mathcal{E}_i, \mathsf{F}_i) \in \mathcal{S}_a$ if it satisfies the properties **[Can read]** and **[Cannot write]**. An encapulation is *confidential*, that is $(\mathcal{E}_i, \mathsf{F}_i) \in \mathcal{S}_c$ if it satisfies the properties **[Cannot read]** and **[Can write]**. Finally, an encapulation is *secure*, that is $(\mathcal{E}_i, \mathsf{F}_i) \in \mathcal{S}_c$ if it satisfies the properties **[Cannot read]** and **[Cannot write]**.

For all ground substitution σ' such that $\mathsf{Tag} \cap st(\sigma') = \emptyset$, if we denote $J = I - i$ then

3. **[Can read]** $[\mathcal{E}_i] \cdot \mathsf{F}_i \vdash \mathsf{t}_{\mathcal{E}_i}$
4. **[Cannot read]** $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ implies $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k \in J} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma \vee \exists x \in \mathsf{X}_{\mathcal{E}_i}.\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k \in J} \vdash x\sigma$

5. **[Can write]** $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$ is equivalent to $\varphi \vee (\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma' \wedge \Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash \mathsf{F}_i\sigma')$
6. **[Cannot write]** $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$ implies either φ or the following property:

$$\exists x \in \mathsf{X}_{\mathcal{E}_i}.\Phi' \vdash x\sigma' \wedge ((\exists j \in N.\mathsf{t}_{\mathcal{E}_i}\sigma' = \mathsf{t}_{\mathcal{E}_j}\sigma \wedge \mathsf{X}_{\mathcal{E}_i}\sigma' \cap \mathsf{X}_{\mathcal{E}_j}\sigma \neq \emptyset) \vee \Phi' \vdash \mathsf{t}_{\mathcal{E}_i}\sigma'))$$

where $\varphi = \exists j \in N.(\mathcal{E}_i \sim \mathcal{E}_j \wedge \mathcal{E}_i\sigma' = \mathcal{E}_j\sigma)$, $N = \{1, \ldots, n\}$ and $\Phi' = \Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I}$.

The set $\mathcal{S}_a$ (resp. $\mathcal{S}_c$, $\mathcal{S}_s$) represents the sets of encapsulations that can be used to implement authentic (resp. confidential, secure) channels. Property 1 indicates that the session keys or their associated public keys cannot be retrieved directly from an encapsulation. Different encapsulations may use for instance the same encryption scheme. However, Property 2 prevents a part of an encapsulation to be mistaken as session key for another encapsulation. Properties 3 to 6 model the access control of an encapsulation. In particular, the term $\mathsf{t}_\mathcal{E}$ of an encapsulation allowing reading access can be derived from the encapsulation $\mathcal{E}$ and its public keys F (Property 3). On the other hand, the term $\mathsf{t}_\mathcal{E}$ of an encapsulation not allowing reading access should not be derived from the encapsulation without knowing the session keys $\mathsf{X}_\mathcal{E}$ (Property 4). Property 5 indicates that an encapsulation allowing writing access can be deduced only if it was already sent on the network (expressed by formula φ) or by generating it from its public keys F and the term $\mathsf{t}_\mathcal{E}$ encapsulated. Lastly, Property 6 models that an encapsulation not allowing writing access cannot be generated by an attacker unless already given or unless some of the session keys in $\mathsf{X}_\mathcal{E}$ are known. In the latter, Property 6 also states that when the term $\mathsf{t}_\mathcal{E}$ is not known to the attacker then he must have extracted it from encapsulations previously received.

Most common encapsulations satisfy the requested properties.

▶ **Theorem 8.** *The following encapsulations are:*

authentic: $\mathcal{E}_{\mathsf{sign}} = \mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x\rangle, x_1)$ *and* $\mathcal{E}_{\mathsf{mac}} = \langle x, \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x, x_1\rangle)\rangle$*;*
confidential: $\mathcal{E}_{\mathsf{aenc}} = \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{aenc}}, x\rangle, \mathsf{pk}(x_1))$*;*
secure: $\mathcal{E}_{\mathsf{TLS}} = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x\rangle, x_1)$, $\mathcal{E}_{\mathsf{BAC}} = \langle t, \mathsf{mac}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, t\rangle, x_2)\rangle$ *with* $t = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x\rangle, x_1)$, *and* $\mathcal{E}_{\mathsf{signcrypt}} = \mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}\mathsf{signcrypt}}, \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{signcrypt}}, x\rangle, \mathsf{pk}(x_1))\rangle, x_2)$.

where $\mathsf{a}_{\mathcal{E}\mathsf{sign}}, \mathsf{a}_{\mathcal{E}\mathsf{mac}}, \mathsf{a}_{\mathcal{E}\mathsf{aenc}}, \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \mathsf{a}_{\mathcal{E}\mathsf{signcrypt}}$ *are constants.*

Moreover, the set $\{(\mathcal{E}_{\mathsf{sign}}, \{\mathsf{vk}(x_1)\}), (\mathcal{E}_{\mathsf{mac}}, \emptyset), (\mathcal{E}_{\mathsf{aenc}}, \{\mathsf{pk}(x_1)\}), (\mathcal{E}_{\mathsf{TLS}}, \emptyset), (\mathcal{E}_{\mathsf{BAC}}, \emptyset), (\mathcal{E}_{\mathsf{signcrypt}}, \emptyset)\}$ *allowsfor authentic, confidential and secure channels.*

The proof of Theorem 8 is available in Appendix B. In the rest of this paper, we assume the existence of a set of encapsulations $\mathcal{S}_e$ allowing authentic, secure and confidential channels.

3.2 Composition of protocols

Encapsulations use session keys, which are established by a key exchange protocol. To express the requested property of this protocol, we need to annotate it with events that specify which keys are established for which channels and agents. Considering a context of channel and agent declarations C and a set of channels S, we denote by $C|_{\overline{S}}$ the context C where all $\mathsf{new}_{ta}\ c$ with $c \in S$ are removed. We denote by $T_{\mathcal{A}gt}$ the set of tuples of agents. We consider special events $\mathsf{Ev} = \{\mathsf{ev}_1, \mathsf{ev}_2, \ldots \in \mathcal{E}v\}$.

▶ **Definition 9.** Let $P = C[R_1, \ldots, R_n]$ be a process with C an agent and channel declaration context such that $R_1, \ldots, R_n$ are roles of agents $A_1, \ldots, A_n$ respectively. Let S be a set of channels such that $channels(C) \cap S = \emptyset$. Let ρ be a mapping from S to $T_{\mathcal{A}gt} \times \mathcal{S}_e$. We say that a process $\tilde{P}$ is an annotation of P under ρ if $\tilde{P} = C[R'_1, \ldots, R'_n]$ where for all $i \in \{1, \ldots, n\}$,

$$R'_i = R_i.\mathsf{event}_{A_i}(\mathsf{ev}_i(c_1, ta_1, ts_1, tp_1)).\ldots.\mathsf{event}_{A_i}(\mathsf{ev}_i(c_m, ta_m, ts_m, tp_m))$$

where $\{c_1, \ldots, c_m\} = \{c \in dom(\rho) \mid c\rho = (ta, (\mathcal{E}, \mathsf{F})) \wedge A_i \in st(ta)\}$ and $\forall j \in \{1, \ldots, m\}$, $c_j\rho = (ta_j, (\mathcal{E}, \mathsf{F}))$, $ts_j = (u_1, \ldots, u_{|\mathsf{X}_\mathcal{E}|})$, $tp = \mathsf{F}(u_1, \ldots, u_{|\mathsf{X}_\mathcal{E}|})$ for some $(\mathcal{E}, \mathsf{F})$ and terms $u_1, \ldots, u_{|\mathsf{X}_\mathcal{E}|}$ such that if $c \in Ch_a$ (resp. Ch_c, Ch_s) then $(\mathcal{E}, \mathsf{F})$ allows authentic (resp. confidential, secure) channels.

At the end of each role R_i, we add the events ev_i for the channels $c_1, \ldots, c_m$ that the agent is supposed to establish. Events $\mathsf{ev}_i(c, ta, ts, tp)$ are composed of four elements: a channel c that the agent wants to instantiate, a tuple of agents ta indicating who is sharing the channel c, a tuple of session keys ts that will be used in the encapsulation $(\mathcal{E}, \mathsf{F})$ to implement c, and lastly a tuple tp of public keys associated to the session keys and F. Typically, we will require that the session keys in ts remain secret for honest agents while the public keys are indeed public.

▶ **Example 10.** Continuing Example 4 and thanks to Theorem 8, the encapsulation $(\mathcal{E}_{\mathsf{BAC}}, \emptyset)$ provides the passport and reader with a secure channel, denoted $c_s \in Ch_s$, once BAC has been executed. The fact that BAC is supposed to establish a secure channel for P and R is expressed by the mapping $\rho = \{c_s \to ((\mathsf{P}, \mathsf{R}), (\mathcal{E}, \emptyset))\}$. The corresponding annotation of BAC under ρ is as follows:

$$\begin{aligned} \tilde{BAC} = \quad & C_{BAC}[R_{\mathsf{P}}.\mathsf{event}_{\mathsf{P}}(\mathsf{ev}_1(c_s, (\mathsf{P}, \mathsf{R}), (\mathsf{f}_1(y, k_{\mathsf{P}}), \mathsf{f}_2(y, k_{\mathsf{P}})))) \\ & \mid R_{\mathsf{R}}.\mathsf{event}_{\mathsf{R}}(\mathsf{ev}_2(c_s, (\mathsf{P}, \mathsf{R}), (\mathsf{f}_1(k_{\mathsf{R}}, w), \mathsf{f}_2(k_{\mathsf{R}}, w))))] \end{aligned}$$

where $C_{BAC}[\_] = \mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}], data[\mathsf{P}]\}).\_$. Note that the session keys are different and reflect the respective views on the session keys of the passport and the reader.

▶ **Definition 11.** Let C and C' be two channel and agent declaration contexts. We say that C and C' are composable if there exist contexts C_1, C_2, C_1', C_2' such that C_1 and C_1' are sequences of agent declarations with $ba(C_1) \cap ba(C_1') = \emptyset$, $C = C_1[C_2]$, $C' = C_1'[C_2']$ and C_2, C_2' only differ from the content of $\mathcal{K}_{pub}, \mathcal{K}_{prv}$ in the instances of $\mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub}, \mathcal{K}_{prv})$.

We define their composition, denoted $\mathsf{C}^{C,C'}$, as the context $C_1[C_1'[C_3]]$ with C_3 being the context C_2 where all instances of $\mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub}, \mathcal{K}_{prv})$ are replaced by $\mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub} \cup \mathcal{K}_{pub}{}', \mathcal{K}_{prv} \cup \mathcal{K}_{prv}{}')$ and $\mathsf{ag}(A, \mathcal{A}, \mathcal{K}_{pub}{}', \mathcal{K}_{prv}{}')$ is in C_2'.

The composability of the channel and agent declaration contexts ensures that the roles of the process Q can be sequentially composed with the roles of the process P. For instance, they should have similar replications, agent declarations or even channel declarations. However, we do not require that an agent in P and Q to have the same private ($\mathcal{K}_{prv}$) or public ($\mathcal{K}_{pub}$) data. We also allow an agent to be declared in one context but not in the other one if declared upfront.

▶ **Example 12.** One of the protocols that are executed after BAC is the Passive Authentication protocol which provides an authentication mechanism proving that the content of the RFID chip is authentic. In fact the ICAO standard also indicates that the chip must contain a signature by the Document Signer authority (D) of a hash of the private data $data[\mathsf{P}]$, $sod \stackrel{def}{=} \mathsf{sign}(\langle \mathsf{a}, \mathsf{h}(\langle \mathsf{a}, data[\mathsf{P}] \rangle) \rangle, sk[\mathsf{D}])$. During the Passive Authentication protocol, after receiving on the secure channel a challenge from the reader, the passport sends back this signature that is checked by the reader.

$$\mathsf{R} \to_{sec} \mathsf{P} : \mathsf{read}$$
$$\mathsf{P} \to_{sec} \mathsf{R} : \langle data, \mathsf{sign}(\langle \mathsf{a}, \mathsf{h}(\langle \mathsf{a}, data \rangle) \rangle, sk)$$

where sk is the signing key of the Document Signer authority. In our calculus, the roles of the reader (Q_{R}) and of the passport (Q_{P}) can be described as follows:

$$\begin{aligned} Q_{\mathsf{P}} = \quad & \mathsf{in}_{\mathsf{P}}(c_s, \mathsf{read}).\mathsf{out}_{\mathsf{P}}(c_s, \langle data[\mathsf{P}], sod \rangle) \\ Q_{\mathsf{R}} = \quad & \mathsf{out}_{\mathsf{R}}(c_s, \mathsf{read}).\mathsf{in}_{\mathsf{R}}(c_s, \langle x', \mathsf{sign}(\langle \mathsf{a}, \mathsf{h}(\langle \mathsf{a}, x' \rangle) \rangle, sk[\mathsf{D}]) \rangle) \end{aligned}$$

The complete representation of the system is given by $PA = C_{PA}[\mathsf{new}\ c_s.(Q_P \mid Q_R)]$ where C_{PA} is the following context:

$$C_{PA} = \mathsf{ag}(\mathsf{D}, \{\mathsf{D}\}, \{\mathsf{vk}(sk[\mathsf{D}])\}, \{sk[\mathsf{D}]\}).\mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{data[\mathsf{P}]\}).\_$$

Continuing Example 10, C_{PA} and C_{BAC} are composable and $\mathsf{C}^{C_{PA}, C_{BAC}}$ is the context:

$$\mathsf{C}^{C_{PA}, C_{BAC}} = \mathsf{ag}(\mathsf{D}, \{\mathsf{D}\}, \{\mathsf{vk}(sk[\mathsf{D}])\}, \{sk[\mathsf{D}]\}).\mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}], data[\mathsf{P}]\}).\_$$

Let S be a set of channels. Let ρ be a mapping from S to $T_{\mathcal{A}gt} \times \mathcal{S}_e$. We say that two processes P and Q are *composable under* ρ if $P = C[R_1, \ldots, R_n]$, $Q = C'[R_1', \ldots, R_n']$ where R_i, R_i' are roles of the

same agent A_i for $i = 1 \dots n$, C and $C'|_{\overline{S}}$ are composable and for all $c \in dom(\rho)$, if $c\rho = (ta, (\mathcal{E}, \mathsf{F}))$ then for all $i \in \{1, \dots, n\}$, $c \in ch_{A_i}(Q)$ is equivalent to $A_i \in ta$. This reflects the fact that agents using channel c should be explicitly listed as authorized agents for c.

The composability between P and Q ensures that the agents in Q sharing abstract authentic, confidential and secure channels are correctly represented in ρ.

▶ **Definition 13.** Let S be a set of channels. Let ρ be a mapping from S to $T_{\mathcal{A}gt} \times \mathcal{S}_e$. Let $P = C[R_1, \dots, R_n]$ and $Q = C'[R'_1, \dots, R'_n]$ two closed composable processes under ρ.

For all $\tilde{P} = C[\tilde{R}_1, \dots, \tilde{R}_n]$ annotations of P under ρ, the implementation of Q by $\tilde{P}$ through ρ, denoted $\tilde{P} \triangleleft^{\rho} Q$, is the process $C_0[R_1.R''_1, \dots, R_n.R''_n]$ where $C_0 = \mathsf{C}^{C,C'|_{\overline{S}}}$ and for all $i \in \{1, \dots, n\}$, R''_i is defined as R'_i where all instances of $\mathsf{out}_A(c, u)$ (resp. $\mathsf{in}_A(c, u)$) are replaced by $\mathsf{out}_A(c_{pub}, \mathcal{E}\sigma)$ (resp. $\mathsf{in}_A(c_{pub}, \mathcal{E}\sigma)$) when $c\rho = (ta, (\mathcal{E}, \mathsf{F}))$, $\mathsf{t}_{\mathcal{E}}\sigma = u$ and $\mathsf{event}_A(\mathsf{ev}_i(c, ta, \mathsf{X}_{\mathcal{E}}\sigma, \mathsf{F}\sigma))$ is in $\tilde{R}_i$ for some substitution σ.

▶ **Example 14.** Continuing Example 12, the implementation of PA by $B\tilde{A}C$ through ρ is thus the process $B\tilde{A}C \triangleleft^{\rho} PA = \mathsf{C}^{C_{PA}, C_{BAC}}[R_P.Q'_P \mid R_R.Q'_R]$ where Q'_P and Q'_R are defined as follows:

$$Q'_{\mathsf{P}} = \mathsf{in}_{\mathsf{P}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\mathsf{read}, K_1, K_2)).\mathsf{out}_{\mathsf{P}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\langle data[\mathsf{P}], sod\rangle, K_1, K_2))$$
$$Q'_{\mathsf{R}} = \mathsf{out}_{\mathsf{R}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\mathsf{read}, K'_1, K'_2)).\mathsf{in}_{\mathsf{R}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\langle x, \mathsf{sign}(\langle \mathsf{a}, \mathsf{h}(\langle \mathsf{a}, x\rangle)\rangle, sk[\mathsf{D}])\rangle, K'_1, K'_2))$$

with $K_1 = \mathsf{f}_1(y, k_{\mathsf{P}})$, $K_2 = \mathsf{f}_2(y, k_{\mathsf{P}})$, $K'_1 = \mathsf{f}_1(k_{\mathsf{R}}, w)$, $K'_2 = \mathsf{f}_2(k_{\mathsf{P}}, w)$. Note that the ICAO standard describes in fact the Passive Authentication protocol as the process $C[Q'_P \mid Q'_R]$ (without tags). Thanks to our result, we may study the simpler process $C[\mathsf{new}\ c_s.(Q_P \mid Q_R)]$.

4 Security property

It is easy to state secrecy in our formalism, using a special event $\mathsf{Sec} \in \mathcal{E}v$: any term occurring in a Sec event should remain secret unless the corresponding session involves a dishonest agent.

▶ **Definition 15.** Let Q be closed process containing contains some events of the form $\mathsf{Sec}(t, (A_1, \dots, A_n))$ where t is a term and $A_1, \dots, A_n$ are some agents. Let Φ be a closed frame. We say that Q preserves secrecy if for all $(Q, \emptyset, \emptyset, \emptyset) \xrightarrow{ev_1 \cdot \dots \cdot ev_m} (Q', \Phi', \mu', \theta')$, for all $i \in \{1, \dots, n\}$, if $ev_i = \mathsf{Sec}(t', (A'_1, \dots, A'_n))$ for some t' and some honest agents $A'_1, \dots, A'_n$ then $\Phi' \nvdash t'$.

We may also specify the properties requested from a key exchange protocol P: P should preserve the secrecy of the session keys occurring in its events and should ensure that the associated public keys are public. Moreover, P also needs to ensure that a session key cannot be used to implement two different channels and that honest agents sharing a channel will share the same session keys for this channel. In such a case, we say that P is a *secure channel establishment protocol*.

▶ **Definition 16.** Let $P = C[R_1, \dots, R_n]$ be a closed process. Let $\tilde{P}$ be an annotation of P under some mapping ρ. We say that $\tilde{P}$ is a *secure channel establishment protocol* when for all $(\tilde{P}, \emptyset, \emptyset, \emptyset) \xrightarrow{e_1 \cdot \dots \cdot e_m} (P', \Phi', \mu', \theta')$, for all $i \in \{1, \dots, m\}$, if $e_i = ev(c, ta, (s_1, \dots, s_\ell), (u_1, \dots, u_q))$ such that $ev \in \mathsf{Ev}$, all agents in ta are honest then for all $k \in \{1, \dots, \ell\}$, $\Phi' \nvdash s_k$ and for all $k \in \{1, \dots, q\}$, $\Phi' \vdash u_k$. Moreover, for all $j \in \{1, \dots, m\}$, if $ev_j = ev'(c', ta', (s'_1, \dots, s'_{\ell'}), (u'_1, \dots, u'_{q'}))$ for some $ev' \in \mathsf{Ev}$, some channel c', some tuple ta' of agents and some tuples $(s'_1, \dots, s'_{\ell'})$ and $(u'_1, \dots, u'_{q'})$ of terms then

- either $ta \neq ta'$ or $c \neq c'$ or $ev = ev'$ implies $\forall k \in \{1, \dots, \ell\}, \forall k' \in \{1, \dots, \ell'\}, s_k \neq s'_{k'}$
- or one of the two following properties is satisfied :
  - $(s_1, \dots, s_\ell) = (s'_1, \dots, s'_{\ell'})$ and $(u_1, \dots, u_q) = (u'_1, \dots, u'_{q'})$.
  - $\forall k \in \{1, \dots, \ell\}, \forall k' \in \{1, \dots, \ell'\}, s_k \neq s'_{k'}$.

The first item indicates that the session keys used for a channel between some honest agents are necessarily different from session keys used for a different channel between any kind of agents, whether they are honest, dishonest or a mix of both. The second item requires that for matching channels and sets of agents, either the session keys perfectly match or they are all different.

We are now ready to state our main result: if P is a secure channel establishment protocol and if Q preserves secrecy using some secure, confidential, or authentic channels, then Q may safely use P to implement its channels. The proof of Theorem 17 is available in a companion report [5].

▶ **Theorem 17.** *Let* tag_A *and* tag_B *be two disjoint sets of tags. Let* $\mathcal{S}_e$ *be a set of* tag_A*-encapsulation allowing authentic, confidential, and secure channels. Let* ρ *be a mapping from channels to* $T_{\mathcal{A}gt} \times \mathcal{S}_e$*. Let* P *and* Q *be two closed executable composable* tag_B*-processes under* ρ *such that* P *and* Q *do not share names and* $fa(P) = fa(Q) = \emptyset$*. Let* $\tilde{P}$ *be an annotation of* P *under* ρ*. If* $\tilde{P}$ *is secure and* Q *preserves secrecy then* $\tilde{P} \cdot^{\rho} Q$ *preserves secrecy as well.*

For simplicity, we prove secure composition w.r.t. secrecy properties but we believe that our result could be easily extended to trace properties.

Sketch of proof. The proof first relies on that fact that the reachability properties are preserved by disjoint parallel composition. In particular, the process $\tilde{P} \mid Q$ is a secure channel establishment protocol and preserves secrecy. The rest of the proof consists in showing that any trace of $\tilde{P} \cdot^{\rho} Q$ is also a trace of $\tilde{P} \mid Q$ with a frame that induces a similar attacker knowledge. More specifically, properties from Definition 7 ensure that tag_B-terms generated by the attacker or obtained from the encapsulations in $\tilde{P} \cdot^{\rho} Q$ do not give any relevant knowledge to the attacker and can be replaced by fresh names. This allows us to obtain a trace without tag_B-terms and so without encapsulations. Lastly, since $\tilde{P} \mid Q$ is a secure channel establishment protocol, we can always match two encapsulations having same session keys with the corresponding abstract channel in $\tilde{P} \mid Q$. ◀

▶ **Example 18.** Continuing Example 14, the annotation under ρ of the Basic Access Control $\tilde{BAC}$ is secure and the Passive Authentication $C_{PA}[\mathsf{new}\ c_s.(Q_P.\mathsf{event}_{\mathsf{P}}(\mathsf{Sec}(data[\mathsf{P}], (\mathsf{P}, \mathsf{R}))) \mid Q_R)]$ preserves secrecy (of the private data). Hence, thanks to Theorems 8 and 17, the implementation of PA by $\tilde{BAC}$ through ρ, $\mathsf{C}^{C_{PA}, C_{BAC}}[R_P.Q'_P.\mathsf{event}_{\mathsf{P}}(\mathsf{Sec}(data[\mathsf{P}], (\mathsf{P}, \mathsf{R}))) \mid R_R.Q'_R]$, preserves secrecy.

5 Case studies

We show that our approach can be applied to deployed protocols such as the biometric passport or TLS applied to 3D-secure. As an application, we show that the automatic analysis through the CL-Atse tool can be significantly speed up when the number of sessions goes higher.

5.1 Biometric passport

Our running example is the combination of the Basic Access Control (BAC) protocol with the Passive Authentication (PA) protocol from the electronic passports. Actually, PA is not the only protocol executed after BAC. Another authentication mechanism is used to prevent cloning of the passport chip. This protocol, called *Active Authentication protocol* (AA), also uses the same session keys and encapsulations than PA. Using the CL-Atse tool [18], we show for different scenarios that BAC is a secure channel establishment protocol and that PA and AA both preserve secrecy. Thanks to our main result, this yields security of the combined protocol, where BAC implements the secure channel of PA and AA. For comparaison purpose, we also analyze directly the combined protocol with CL-Atse. These analysis are reported in Section 5.3

5.2 TLS and 3D-secure

Our results also apply to other complex systems. We study the *Visa 3D-secure protocol* [17] used by several websites for internet banking and that relies on secure channels implemented by the well known TLS protocol. The Visa 3D secure protocol is an authenticated payment method between a card holder and a merchant during an electronic payment. This protocol aims to ensure authentication of the card holder as well as confirmation that the card holder is authorized by his bank to make the payment. Lastly, the protocol also aims to ensure the secrecy of the card holder's banking information, the payment amount and other data.

The protocol involves four types of participants: a card holder (C), a merchant (M), a centralized structure called Visa Directory Servers (DS) and the card issuer's servers called Access Control Servers (ACS). The main role of the Visa Directory Servers is to transfer card holder's information between the Access Control Servers and the merchant. In itself, the 3D secure protocol is already a complex protocol with multiple exchanges of messages. But the protocol also requires most messages to be exchanged trough a TLS channel. More specifically, messages of the 3D secure protocol shall be encrypted with a symmetric session key previously established with TLS. In our model, this means that the messages are encapsulated by $(\mathcal{E}_{\mathsf{TLS}}, \emptyset)$, as defined in Theorem 8.

The well known TLS protocol [15, 9] aims at establishing a secure channel between a client and a server. Using the CL-Atse tool, we show that TLS (Basic TLS handshake, in the RSA mode) is indeed a secure channel establishment protocol.

Note that for one session of the Visa 3D secure protocol yields four sessions of the TLS protocol: one channel between C and M, between C and ACS, between ACS and DS and finally between M and DS. This renders the verification of even one session of 3D secure protocol with the channels implemented by TLS a complex task (more than thirty five messages exchanged per session).

5.3 Analysis with CL-Atse

We applied the automatic verification tool CL-Atse [18] on a Dell T1700 computer (16 Go RAM, 3.40 GHz CPU). The corresponding time of analysis are displayed below.

		Computation time (in seconds, timeout set to 24 hours)							
protocols		TLS & 3D secure		BAC & PA		BAC & AA		BAC & PA & AA	
complete system (C) or separated analysis (S)		S	C	S	C	S	C	S	C
number of sessions considered	1	0.2	0.1	0.7	0.1	0.7	0.1	0.7	0.2
	2	1350	time out	6.2	1.6	6.2	1.6	6.5	43156
	3	time out	time out	9133	time out	9133	time out	9185	time out

Amongst the tools able to verify security protocols for a bounded number of sessions, CL-Atse is well known and considered to be one of the fastest. However, in the case of the 3D-secure protocol, the tool already fails to verify one session with all channels implemented as we reached a time out set to 24 hours of computation. Thus, to obtain meaningful results with the 3D-secure protocol, we considered the case where only the channel between the card holder and the merchant is implemented. Already in this case, we can see a clear benefit from analyzing separately 3D-secure and TLS when considering two sessions. Indeed, the verification can be performed under 25 minutes when analysing the protocols separately whereas the tool was reaching a time out when considering the complete system. We obtain similar results with the Basic Access Control protocol, the Active Authentication protocol and the Passive Authentication protocol. Note that for verification tools handling unbounded number of sessions (*e.g.* ProVerif [3], Tamarin [14]), the gain in time would probably be less significant since these tools do not systematically explore all interleavings.

6 Conclusion

We have shown how to securely compose a protocol with the implementation of its channels. We have provided a characterization for the three most common types of channels: secure, confidential, and authentic channels. We plan to consider other types of communication channels like anonymous channels. This will certainly require to extend our approach to equivalence properties.

Our composition result holds for a class of primitives that encompasses all standard cryptographic primitives. We plan to extend it to a larger class of primitives, including in particular exclusive or or homomorphic encryption.

Our result assumes a light tagging of the primitives, to ensure that an encapsulation cannot be confused with a message coming from the protocols. While tagging is reasonable, it is not often done in practice. On the other hand standard protocols typically enjoy some non unifiability properties that prevent such confusion. We believe that our result could be extended to a general notion of non unifiability of the terms, without having to require explicit tagging.

Acknowledgments:

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 258865, project ProSecure.

References

1 Machine readable travel document. Technical Report 9303, International Civil Aviation Organization, 2008.

2 M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. of the 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, January 2001.

3 B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proc. CSFW'01*, 2001.

4 B. Blanchet and A. Podelski. Verification of cryptographic protocols: Tagging enforces termination. In A. Gordon, editor, *Foundations of Software Science and Computation Structures (FoSSaCS'03)*, volume 2620 of *LNCS*, April 2003.

5 V. Cheval, V. Cortier, and E. Le-Morvan. secure refinements of communication channels. research report RR-8790, Inria, eric.le-morvan@inria.fr, 2015.

6 Ş. Ciobâcă and V. Cortier. Protocol composition for arbitrary primitives. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 322–336, Edinburgh, Scotland, UK, July 2010. IEEE Computer Society Press.

7 V. Cortier and S. Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1):1–36, Feb. 2009.

8 A. Datta, A. Derek, J. C. Mitchell, and A. Roy. Protocol composition logic (PCL). *Electr. Notes Theoretical Computer Science*, 172:311–358, 2007.

9 T. Dierks and E. Rescorla. The transport layer security (tls) protocol version 1.2 (rfc 5246). Technical report, IETF, 2008.

10 T. Gibson-Robinson, A. Kamil, and G. Lowe. Verifying layered security protocols. *Journal of Computer Security*, 23(3), 2015.

11 J. D. Guttman. Authentication tests and disjoint encryption: a design method for security protocols. *Journal of Computer Security*, 12(3–4):409–433, 2004.

12 J. D. Guttman. Establishing and preserving protocol security goals. *Journal of Computer Security*, 22(2):203–267, 2004.

13 J. D. Guttman and F. J. Thayer. Protocol independence through disjoint encryption. In *Proc. 13th Computer Security Foundations Workshop (CSFW'00)*, pages 24–34. IEEE Comp. Soc. Press, 2000.

14 S. Meier, B. Schmidt, C. Cremers, and D. Basin. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In N. Sharygina and H. Veith, editors, *Computer Aided Verification, 25th International Conference, CAV 2013, Princeton, USA, Proc.*, volume 8044 of *Lecture Notes in Computer Science*, pages 696–701. Springer, 2013.

15 C. Meyer and J. Schwenk. Lessons learned from previous ssl/tls attacks : A brief chronology of attacks and weaknesses. In *IACR Cryptology ePrint*, 2013.

16 S. Moedersheim and L. Viganò. Sufficient conditions for vertical composition of security protocols. In *ASIACCS*, pages 435–446, 2014.

17 V. Pasupathinathan, J. Pieprzyk, H. Wang, and J. Y. Cho. Formal analysis of card-based payment systems in mobile services. In *Fourth Australian information security workshop, conferences in research and practise in information security*, pages 213–220, 2006.

18 M. Turuani. The CL-Atse Protocol Analyser. In *Term Rewriting and Applications - Proc. of RTA*, volume 4098 of *Lecture Notes in Computer Science*, pages 277–286, Seattle, WA, USA, 2006.

A Modelization of other protocols

A.1 TLS and 3D secure

A.1.1 TLS

TLS is the protocol that is most often used when an application needs a secure channel to communicate on a public network. In a TLS session between a client C and a server S, C and S start by doing a handshake : C sends a message containing a constant helloC along with his name, a session number id and a fresh nonce n_C. The server then answers a constant helloS along with the same session number id, another fresh nonce n_S and its signed public encryption key. After that, C runs the key exchange step by encrypting with S's public key a message containing a randomly generated value pms along with the two previous nonces n_C and n_S, S checks that n_C and n_S are in the message he received and if so C and S build the session key $\mathsf{keygen}(pms, n_S, n_C)$. The two last steps consist in C and S sending each other respectively the hashes $finishC$ and $finishS$ encrypted by $\mathsf{keygen}(pms, n_S, n_C)$: they contain all the values that were transmitted during the session, furthermore $finishC$ and $finishS$ contain respectively the labels client and server so that they can not be confused. $finishC$ and $finishS$ enable C and S to check that they agree upon what has been transmitted during the session. The session key $\mathsf{keygen}(pms, n_S, n_C)$ provided by TLS will be used to implement the channels in other protocols

Here is diagram showing how a TLS session works with $\mathsf{t_{TLS}}$ a tag:

$$
\begin{aligned}
&C \to S : \langle \mathsf{helloC}, name[C], n_C, id\rangle\\
&S \to C : \langle \mathsf{helloS}, n_S, id\rangle\\
&S \to C : \mathsf{sign}(\langle \mathsf{t_{TLS}}, name[S], \mathsf{pk}(priv[S])\rangle, sk[S])\\
&C \to S : \mathsf{aenc}(\langle \mathsf{t_{TLS}}, pms\rangle, \mathsf{pk}(priv[S]))\\
&C \to S : \mathsf{senc}(\langle \mathsf{t_{TLS}}, finishC\rangle, \mathsf{keygen}(pms, n_C, n_S))\\
&\quad \text{with } finishC = \mathsf{h}(\langle \mathsf{t_{TLS}}, \mathsf{keygen}(pms, n_C, n_S), name[C], name[S], n_C, n_S, id, \mathsf{client}\rangle)\\
&S \to C : \mathsf{senc}(\langle \mathsf{t_{TLS}}, finishS\rangle, \mathsf{keygen}(pms, n_C, n_S))\\
&\quad \text{with } finishS = \mathsf{h}(\langle \mathsf{t_{TLS}}, \mathsf{keygen}(pms, n_C, n_S), name[C], name[S], n_C, n_S, id, \mathsf{server}\rangle)
\end{aligned}
$$

In our models, the roles of the client (R_{C}) and of the server (R_{S}) are as follows, with $c \in Ch_p$:

$$
\begin{aligned}
R_{\mathsf{C}} = \;& \mathsf{new}\ n_C.\mathsf{new}\ id.\mathsf{out_C}(c, \langle \mathsf{helloC}, name[C], n_C, id\rangle).\mathsf{in_C}(c, \langle \mathsf{helloS}, x, id\rangle).\\
& \mathsf{in_C}(c, \mathsf{sign}(\langle \mathsf{t_{TLS}}, name[S], u\rangle, sk[S])).\mathsf{new}\ pms.\mathsf{out_C}(c, \mathsf{aenc}(\langle \mathsf{t_{TLS}}, pms\rangle, u)).\\
& \mathsf{out_C}(c, \mathsf{senc}(\langle \mathsf{t_{TLS}}, finishC_1\rangle, \mathsf{keygen}(pms, n_C, x))).\\
& \mathsf{in_C}(c, \mathsf{senc}(\langle \mathsf{t_{TLS}}, finishS_1\rangle, \mathsf{keygen}(pms, n_C, x))).0
\end{aligned}
$$

$$
\begin{aligned}
R_{\mathsf{S}} = \;& \mathsf{in_S}(c, \langle \mathsf{helloC}, v, w, y\rangle).\mathsf{new}\ n_S.\mathsf{out_S}(c, \langle \mathsf{helloS}, n_S, y\rangle).\\
& \mathsf{out_S}(c, \mathsf{sign}(\langle \mathsf{t_{TLS}}, name[S], \mathsf{pk}(priv[S])\rangle, sk[S])).\\
& \mathsf{in_S}(c, \mathsf{aenc}(\langle \mathsf{t_{TLS}}, z\rangle, \mathsf{pk}(priv[S]))).\mathsf{in_S}(c, \mathsf{senc}(\langle \mathsf{t_{TLS}}, finishC_2\rangle, \mathsf{keygen}(z, w, n_S))).\\
& \mathsf{out_S}(c, \mathsf{senc}(\langle \mathsf{t_{TLS}}, finishS_2\rangle, \mathsf{keygen}(z, w, n_S))).0
\end{aligned}
$$

where

$$
\begin{aligned}
finishC_1 &= \mathsf{h}(\langle \mathsf{keygen}(pms, n_C, x), name[C], name[S], n_C, x, Id, \mathsf{client}\rangle)\\
finishS_1 &= \mathsf{h}(\langle \mathsf{keygen}(pms, n_C, x), name[C], name[S], n_C, x, Id, \mathsf{server}\rangle)\\
finishC_2 &= \mathsf{h}(\langle \mathsf{keygen}(z, w, n_S), v, name[C], name[S], w, n_S, y, \mathsf{client}\rangle)\\
finishS_2 &= \mathsf{h}(\langle \mathsf{keygen}(z, w, n_S), v, name[C], name[S], w, n_S, y, \mathsf{server}\rangle)
\end{aligned}
$$

The session key provided by TLS is $\mathsf{keygen}(z, w, n_S)$ for R_{S} and $\mathsf{keygen}(pms, n_C, x)$ for R_{C}.

A.1.2 3D secure

An informal description of a *3D-secure* session between a client C, a merchant M, a directory server DS and an access control server ACS is provided below.

$C \rightarrow_{sec} M : \langle pan[C], expiry[C] \rangle$
$M \rightarrow_{sec} DS : \langle pan[C], password[M], infoM \rangle$
$DS \rightarrow_{sec} ACS : \langle pan[C], infoM \rangle$
$ACS \rightarrow_{sec} DS : \langle \mathsf{panok}, acctid, url[ACS], proto \rangle$
$DS \rightarrow_{sec} M : \langle \mathsf{panok}, acctid, url[ACS], proto \rangle$
$M \rightarrow_{sec} C : \mathsf{sign}(\langle \mathsf{t_{3D}}, infoM, publicM, expiry[C], transInfo \rangle, sk_{VISA}[M])$
$C \rightarrow_{sec} ACS : \mathsf{sign}(\langle \mathsf{t_{3D}}, infoM, publicM, expiry[C], transInfo \rangle, sk_{VISA}[M])$
$ACS \rightarrow_{sec} C : \langle name[M], payInfo, panshort[C], expiry[C] \rangle$
$ACS \rightarrow_{outofband} C : pam[C]$
$C \rightarrow_{sec} ACS : password[C]$
$ACS \rightarrow_{sec} C : \mathsf{sign}(\langle \mathsf{t_{3D}}, infoM, xid, payInfo, panshort[C], status, otherInfo \rangle, sk_{VISA}[ACS])$
$C \rightarrow_{sec} M : \mathsf{sign}(\langle \mathsf{t_{3D}}, infoM, xid, payInfo, panshort[C], status, otherInfo \rangle, sk_{VISA}[ACS])$
$M \rightarrow_{sec} C : \mathsf{sign}(\langle \mathsf{t_{3D}}, status \rangle, sk_{VISA}[M])$

where $infoM = \langle macqbin, id[M] \rangle$, $publicM = \langle name[M], url[M] \rangle$, $transInfo = \langle xid, pdate, pamnt, acctid \rangle$, $payInfo = \langle pamnt, pdate \rangle$ and $otherInfo = \langle date, cavv, eci, cavvalg \rangle$. The specification of the 3D-secure protocol is not public, the semantics of some of the data (e.g. *cavv*, *eci*, *cavvalg*) are unspecified even in [17]. That is why in the protocol we model them as nonces.

A 3D-secure session starts when C sends to M a purchase request containing her primary account number $pan[C]$ and the expiration date $expiry[C]$ of the card. Then M forwards to DS $pan[C]$ along with M's identifiers $infoM$ and $password[M]$ shared only by M and DS : M asks for confirmation about C's banking account. DS transmits to ACS the identifiers of M along with $pan[C]$ so that ACS certifies the existence of the bank account of C. Upon successful verification, ACS sends confirmation panok to DS along with its own url $url[ACS]$ and some other information to be forwarded to M. M then sends to C a signed copy of M's own information $infoM$ and $publicM$ along with the identifiers $transInfo$ regarding the transaction, furthermore it makes C initiate a communication with ACS thanks to his knowledge of $url[ACS]$. C forwards M's signed message to ACS so that ACS checks C. ACS sends back to C a summary of the transaction (M's identity, $payInfo$ and $panshort[C]$). ACS also sends a personnal assurance message $pam[C]$ at some point that C uses to determine the password $password[C]$ that she has to give to authentify herself to ACS. The nature of $pam[C]$ is not specified, usually it consists in a secret code sent to C's mobile phone that has to be sent back, or it can be a password matrix given to C when she gets her credit card, in that case C just has to send the password contained in a case specified by ACS. In the end, ACS gives C a signed message containing all the data necessary to conclude the transaction. That certified message is then forwarded to M and finally M signs with his own signing key the *status* of the transaction between C and M.

We notice that the signing key *sk* involved in TLS is different from the ones involved in *3D secure*, which models the fact that signing keys in *3D secure* are provided by VISA that is in charge of credit cards, thus that signing key has no reason to be involved in TLS. Consequently TLS and *3D secure* do not share names, which is a prerequisite of our result.

A.1.3 Composition between TLS and 3D secure

Channels in *3D secure* have to be implemented between all the users that have to speak together, namely C and M, M and DS, DS and ACS, ACS and C. Thus if *3D secure* is to be composed with

TLS, we need to instanciate it with all the agents that will later share secure channels in *3D secure*. However given that the CL-Atse tool can not analyse 4 TLS sessions within a reasonable time (24 hours), we had to restrict the composition to only one channel implementation between C and M. Consequently we model the case where there is only one honest Access Directory Server ACS, one honest Directory Server DS and one honest merchant M speaking with an unbounded number of clients, possibly dishonest. The four roles of *3D-secure* are denoted by R'_{C}, R'_{M}, R'_{DS}, and R'_{ACS}. Thus *3D secure* can be modeled by the following process:

$$3D = C_{3D}[\mathsf{new}\ c_s^{ca_1}.\mathsf{new}\ c_s^{ca_2}.\mathsf{new}\ c_s^{cm}.\mathsf{new}\ c_s^{ma}.\mathsf{new}\ c_s^{ad}.(R'_C \mid R'_M \mid R'_{ACS} \mid R'_{DS})]$$

where

$$C_{3D}[\_] = \mathsf{ag}(M,\{M\},\mathcal{K}'^{M}_{pub},\mathcal{K}'^{M}_{prv}).\mathsf{ag}(ACS,\{ACS\},\emptyset,\mathcal{K}'^{ACS}_{prv}).\mathsf{ag}(DS,\{DS\},\emptyset,\emptyset).!\mathsf{ag}(C,\mathcal{P},\emptyset,\mathcal{K}'^{C}_{prv}).\_$$

with the sets $\mathcal{K}'^{M}_{pub} = \{id[M], name[M]\}$, $\mathcal{K}'^{M}_{prv} = \{password[M], sk_{VISA}[M], url[M]\}$, $\mathcal{K}'^{C}_{prv} = \{pan[C], expiry[C], pam[C], password[C]\}$ and $\mathcal{K}'^{ACS}_{prv} = \{sk_{VISA}[ACS], url[ACS]\}$.

Since we implement only the secure channel between C and M, the complete representation of the system is the process $TLS = \mathsf{ag}(M,\{M\},\mathcal{K}^{M}_{pub},\mathcal{K}^{M}_{prv}).!\mathsf{ag}(C,\mathcal{P},\mathcal{K}^{C}_{pub},\emptyset).(R_{\mathsf{C}} \mid R_{\mathsf{S}})$ where $\mathcal{P}$ is an infinite set of agents containing honest and dishonest agents such that $M \notin \mathcal{P}$ and $\mathcal{K}^{M}_{pub} = \{\mathsf{pk}(priv[M]), \mathsf{vk}(sk[M]), name[M]\}$, $\mathcal{K}^{M}_{prv} = \{priv[M], sk[M]\}$, $\mathcal{K}^{C}_{pub} = \{name[C]\}$.

As previously mentioned, the 3D-secure protocol specifies that all the exchanged messages should be done on secure channels implemented by TLS, except the out of bound channel used by the issuer's Access Control Servers. More specifically, they require that all messages of the 3D secure protocol must be encrypted with a symmetric session key previously established with TLS. In our model, it means that the messages are encapsulated by $(\mathcal{E}_{\mathsf{TLS}},\emptyset)$, as defined in Theorem 8. Moreover as explained in Section 5, the session keys provided by TLS are $\mathsf{keygen}(z,w,n_S)$ and $\mathsf{keygen}(pms,n_C,x)$ for the card holder and merchant respectively. Therefore, by defining the mapping $\rho = \{c_S^{cm} \to ((C,M),(\mathcal{E}_{\mathsf{TLS}},\emptyset))\}$, an annotation of TLS under ρ is the following process:

$$\tilde{TLS} = C_{TLS}[R_{\mathsf{C}}.\mathsf{event}_{\mathsf{C}}(\mathsf{ev}(c_s^{cm},(C,M),k^1_{CM})) \mid R_{\mathsf{S}}.\mathsf{event}_{\mathsf{M}}(\mathsf{ev}(c_s^{cm},(C,M),k^2_{CM}))]$$

where $C_{TLS}[\_] = \mathsf{ag}(M,\{M\},\mathcal{K}^{M}_{pub},\mathcal{K}^{M}_{prv}).\mathsf{ag}(C,\mathcal{P},\mathcal{K}^{C}_{pub},\emptyset).\_$, $k^1_{CM} = \mathsf{keygen}(pms,n_C,x))$ and $k^2_{CM} = \mathsf{keygen}(z,w,n_S))$. Therefore, the implementation of $3D$ by $\tilde{TLS}$ through ρ is the process:

$$\tilde{TLS} \cdot^{\rho} 3D = \mathsf{C}^{C_{TLS},C_{3D}}[(\mathsf{new}\ c_S^{ca_1}.\mathsf{new}\ c_S^{ca_2}.\mathsf{new}\ c_S^{ma}.\mathsf{new}\ c_S^{ad}.(R_{\mathsf{C}}.R'_C) \mid (R_{\mathsf{S}}.R'_M) \mid R'_{ACS} \mid R'_{DS})]$$

where

$$\mathsf{C}^{C_{TLS},C_{3D}}[\_] = \mathsf{ag}(M,\{M\},\mathcal{K}^{M}_{pub}\cup\mathcal{K}'^{M}_{pub},\mathcal{K}^{M}_{prv}\cup\mathcal{K}'^{M}_{prv}).\mathsf{ag}(ACS,\{ACS\},\mathcal{K}'^{ACS}_{pub},\mathcal{K}'^{ACS}_{prv}).\\ \mathsf{ag}(DS,\{DS\},\emptyset,\emptyset).!\mathsf{ag}(C,\mathcal{P},\mathcal{K}^{C}_{pub},\mathcal{K}^{C}_{prv}\cup\mathcal{K}'^{C}_{prv}).\_$$

Our result now enables us to conclude that if

$$C_{3D}[(\mathsf{new}\ c_S^{ca_1}.\mathsf{new}\ c_S^{ca_2}.\mathsf{new}\ c_S^{cm}.\mathsf{new}\ c_S^{ma}.\mathsf{new}\ c_S^{ad}.\\ (R'_C.\mathsf{event}_C(\mathsf{Sec}(pan[C],(C,M,ACS,DS))) \mid R'_M \mid R'_{ACS} \mid R'_{DS}))]$$

preserves secrecy (in that instance, the secrecy of $pan[C]$) and if $\tilde{TLS}$ is secure, then the implementation of the process $3D$ by $\tilde{TLS}$ through ρ preserves secrecy. Furthermore we can also look at the secrecy of other data such as $pam[C]$ expressed as follows.

$$C_{3D}[(\mathsf{new}\ c_S^{ca_1}.\mathsf{new}\ c_S^{ca_2}.\mathsf{new}\ c_S^{cm}.\mathsf{new}\ c_S^{ma}.\mathsf{new}\ c_S^{ad}.\\ (R'_C.\mathsf{event}_C(\mathsf{Sec}(pam[C],(C,ACS))) \mid R'_M \mid R'_{ACS} \mid R'_{DS}))]$$

Note that the secrecy of $pam[C]$ only concerns the agents C and ACS whereas the secrecy of $pan[C]$ is between C, M, ACS, DS. Our model allows us to verify the secrecy of $pam[C]$ even when M or DS can be dishonest.

A.2 Active Authentication protocol

The aim of the Active Authentication protocol (AA) is to prevent cloning of the passport chip. For that purpose the protocol relies on a signing key $sk[\mathsf{P}]$ that is registered in a tempered resistant memory and cannot be read or copied. A certificate of the verification key $\mathsf{vk}(sk[\mathsf{P}])$ provided by the Document Signer authority mentioned in Example 12 is in fact contained in the data of the passport. For sake of simplicity, we represented these data in Example 12 as a name $data[\mathsf{P}]$ since their exact value was irrelevant for the implementation of the Passive Authentication protocol by the Basic Access Control protocol. In reality, the data stored in the chip is organized in data groups (dg_1 up to dg_{19}), some of them containing the passport holder's name, picture, etc. In particular, the certificate of the verification key $\mathsf{vk}(sk[\mathsf{P}])$, that is $\mathsf{sign}(\mathsf{vk}(sk[\mathsf{P}]), sk[\mathsf{D}])$, is stored in the data group dg_{15}. Thus, by replacing, in the Passive Authentication presented in Example 12, the name $data[\mathsf{P}]$ by the tuple of data groups, we can see that a reader would then be able to obtain from d_{15} the verification key $\mathsf{vk}(sk[\mathsf{P}])$ after the execution of the protocol.

A session of the Active Authentication protocol is as follows: R sends to P a nonce n_R that P has to send back along with a nonce n_P after having them signed with $sk[P]$. In our study we consider the case where AA is a-tagged, although it is not the case in practice.

$$\mathsf{R} \rightarrow_{sec} \mathsf{P} : \langle \mathsf{init}, n_R \rangle$$
$$\mathsf{P} \rightarrow_{sec} \mathsf{R} : \mathsf{sign}(\langle \mathsf{a}, n_P, n_R \rangle, sk[P])$$

The AA roles of the reader (Q_{R}) and of the passport (Q_{P}) on $c_s \in Ch_s$ can be expressed as below in our formalism :

$$Q_{\mathsf{R}} = \mathsf{new}\ n_R.\mathsf{out}_{\mathsf{R}}(c_s, \langle \mathsf{init}, n_R \rangle).\mathsf{in}_{\mathsf{R}}(c_s, \mathsf{sign}(\langle \mathsf{a}, x', n_R \rangle, sk[\mathsf{P}]))$$
$$Q_{\mathsf{P}} = \mathsf{in}_{\mathsf{P}}(c_s, \langle \mathsf{init}, y' \rangle).\mathsf{new}\ n_P.\mathsf{out}_{\mathsf{P}}(c_s, \mathsf{sign}(\langle \mathsf{a}, n_P, y' \rangle, sk[\mathsf{P}]))$$

We model the case where one honnest reader speaks with an unbounded number of honest and dishonest passports. Thus AA can be modeled as a whole by $AA = C_{AA}[\mathsf{new}\ c_s.(Q_{\mathsf{R}} \mid Q_{\mathsf{P}})]$ where

$$C_{AA} = \mathsf{ag}(\mathsf{D}, \{\mathsf{D}\}, \mathsf{vk}(sk[\mathsf{D}]), sk[\mathsf{D}]).\mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{sk[\mathsf{P}]\}).\_$$

where $\mathcal{P}$ is an infinite set of agents containing honest and dishonest agents and $\mathsf{R}, \mathsf{D} \notin \mathcal{P}$.

We study the composition between the Basic Access Control (BAC) and AA. As explained in the section 2.3, in the a-tagged BAC protocol the role of the passport (R_{P}) and the role of the reader (R_{R}) can be modeled as shown below, with $c \in Ch_p$, $M = \mathsf{senc}(\langle \mathsf{a}, x, n_{\mathsf{P}}, y \rangle, ke[\mathsf{P}])$, $N = \mathsf{senc}(\langle \mathsf{a}, n_{\mathsf{P}}, x, k_{\mathsf{P}} \rangle, ke[\mathsf{P}])$, $U = \mathsf{senc}(\langle \mathsf{a}, n_{\mathsf{R}}, z, k_{\mathsf{R}} \rangle, ke[\mathsf{P}])$ and $V = \mathsf{senc}(\langle \mathsf{a}, z, n_{\mathsf{R}}, w \rangle, ke[\mathsf{P}])$:

$$R_{\mathsf{P}} = \mathsf{in}_{\mathsf{P}}(c, \mathsf{challenge}).\mathsf{new}\ n_{\mathsf{P}}.\mathsf{out}_{\mathsf{P}}(c, n_{\mathsf{P}}).\mathsf{in}_{\mathsf{P}}(c, \langle M, \mathsf{mac}(\langle \mathsf{a}, M \rangle, km[\mathsf{P}]) \rangle).$$
$$\mathsf{new}\ k_{\mathsf{P}}.\mathsf{out}_{\mathsf{P}}(c, \langle N, \mathsf{mac}(\langle \mathsf{a}, N \rangle, km[\mathsf{P}]) \rangle).0$$

$$R_{\mathsf{R}} = \mathsf{out}_{\mathsf{R}}(c, \mathsf{challenge}).\mathsf{in}_{\mathsf{R}}(c, z).\mathsf{new}\ k_{\mathsf{R}}.\mathsf{new}\ n_{\mathsf{R}}.\mathsf{out}_{\mathsf{R}}(c, \langle U, \mathsf{mac}(\langle \mathsf{a}, U \rangle, km[\mathsf{P}])).$$
$$\mathsf{in}_{\mathsf{R}}(c, \langle V, \mathsf{mac}(\langle \mathsf{a}, V \rangle, km[\mathsf{P}]) \rangle).0$$

Hence an honest reader communicating with an unbounded number of passports that are either honest or dishonest can be modeled by :

$$BAC = \mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}]\}).(R_{\mathsf{P}} \mid R_{\mathsf{R}})$$

As written in section 3.1, the BAC protocol is meant to generate two session keys per role ($\mathsf{f}_1(y, k_{\mathsf{P}})$ and $\mathsf{f}_2(y, k_{\mathsf{P}})$ for R_{P}, $\mathsf{f}_1(k_{\mathsf{R}}, w)$ and $\mathsf{f}_2(k_{\mathsf{R}}, w)$ for R_{R}), and the messages sent in AA are all encapsulated by $(\mathcal{E}_{\mathsf{BAC}}, \emptyset)$ where $\mathcal{E}_{\mathsf{BAC}} = \langle t, \mathsf{mac}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, t \rangle, x_2) \rangle$ with $t = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x \rangle, x_1)$, $\mathsf{t}_{\mathcal{E}_{\mathsf{BAC}}} = x$ and $\mathsf{X}_{\mathcal{E}_{\mathsf{BAC}}} = (x_1, x_2)$. By theorem 8, the encapsulation $(\mathcal{E}_{\mathsf{BAC}}, \emptyset)$ implements secure channels.

The fact that BAC aims at establishing a secure channel for P and R is translated in our model by using the mapping $\rho = \{c_s \to ((\mathsf{P}, \mathsf{R}), (\mathcal{E}_{\mathsf{BAC}}, \emptyset))\}$ and the associated annotation of BAC under ρ:

$$\begin{aligned} \tilde{BAC} = \quad & C_{BAC}[R_{\mathsf{P}}.\mathsf{event}_{\mathsf{P}}(\mathsf{ev}(c_s, (\mathsf{P}, \mathsf{R}), (\mathsf{f}_1(y, k_{\mathsf{P}}), \mathsf{f}_2(y, k_{\mathsf{P}})))) \\ & \mid R_{\mathsf{R}}.\mathsf{event}_{\mathsf{R}}(\mathsf{ev}(c_s, (\mathsf{P}, \mathsf{R}), (\mathsf{f}_1(k_{\mathsf{R}}, w), \mathsf{f}_2(k_{\mathsf{R}}, w))))] \end{aligned}$$

where $C_{BAC}[\_] = \mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}]\}).\_$.

Hence the two contexts C_{BAC} and C_{AA} can be composed into the new context

$\mathsf{C}^{C_{AA}, C_{BAC}} = \mathsf{ag}(\mathsf{D}, \{\mathsf{D}\}, \mathsf{vk}(sk[\mathsf{D}]), sk[\mathsf{D}]).\mathsf{ag}(\mathsf{R}, \{\mathsf{R}\}, \emptyset, \emptyset).!\mathsf{ag}(\mathsf{P}, \mathcal{P}, \emptyset, \{ke[\mathsf{P}], km[\mathsf{P}], sk[\mathsf{P}]\}).\_$

And now we can write the process $\tilde{BAC} \cdot^{\rho} PA = \mathsf{C}^{C_{AA}, C_{BAC}}[R_P.Q'_P \mid R_R.Q'_R]$ where Q'_P and Q'_R are defined as follows:

$$\begin{aligned} Q'_{\mathsf{P}} = \quad & \mathsf{in}_{\mathsf{P}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\langle \mathsf{init}, y' \rangle, K_1, K_2)). \\ & \mathsf{new}\ n_P.\mathsf{out}_{\mathsf{P}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\mathsf{sign}(\langle \mathsf{a}, n_P, y' \rangle, sk[\mathsf{P}]), K_1, K_2)) \\ Q'_{\mathsf{R}} = \quad & \mathsf{new}\ n_R.\mathsf{out}_{\mathsf{R}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\langle \mathsf{init}, n_R \rangle, K'_1, K'_2)). \\ & \mathsf{in}_{\mathsf{R}}(c_{pub}, \mathcal{E}_{\mathsf{BAC}}(\mathsf{sign}(\langle \mathsf{a}, x', n_P \rangle, sk[\mathsf{P}]), K'_1, K'_2)) \end{aligned}$$

with $K_1 = \mathsf{f}_1(y, k_{\mathsf{P}})$, $K_2 = \mathsf{f}_2(y, k_{\mathsf{P}})$, $K'_1 = \mathsf{f}_1(k_{\mathsf{R}}, w)$, $K'_2 = \mathsf{f}_2(k_{\mathsf{P}}, w)$.

Our result enables us for instance to conclude that if the annotation under ρ of the Basic Access Control $\tilde{BAC}$ is secure and if the Active Authentication

$$C_{AA}[\mathsf{new}\ c_s.(Q_{\mathsf{R}} \mid Q_{\mathsf{P}}.\mathsf{event}_{\mathsf{P}}(\mathsf{Sec}(sk[P], (P))))]$$

preserves secrecy, then

$$\mathsf{C}^{C_{AA}, C_{BAC}}[R_P.Q'_P.\mathsf{event}_{\mathsf{P}}(\mathsf{Sec}(sk[P], (P))) \mid R_R.Q'_R]$$

also preserves secrecy.

B Secure encapsulations

For our proofs, we will need to discuss about the deduction proof of $\Phi \vdash t$. As such, we will denote by $\Phi \vdash_P t$ the deduction of $\Phi \vdash t$ with an associated proof P. We write $\Phi \vdash_i t$ when t is the i-th element of Φ. We write $\Phi \vdash_t t$ when $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$. When an inference rule ir is applied on premises $\Phi \vdash_{P_1} u_1, \ldots, \Phi \vdash_{P_n} u_n$ to obtain the term u, we write $\Phi \vdash_{\mathsf{ir}(P_1, \ldots, P_n)} u$. Note that given a proof P and a frame Φ, there exists a unique t such that $\Phi \vdash_P t$.

Given as a proof P can be seen as a term, we write $\mathcal{M}(P) = (n, m)$ the pair of integer where $n = \max\{i \in st(P) \cap \mathcal{N}\}$ if $st(P) \cap \mathcal{N} \neq \emptyset$ else $n = 0$; and $m = |P|$ where $|P|$ is the number of symbols in P. We also consider the lexicographic order on pairs of integers. Given Φ and t, we say that a proof P of $\Phi \vdash t$ is minimal for $\mathcal{M}$ if for all P', $\Phi \vdash_{P'} t$ implies $\mathcal{M}(P) \leq \mathcal{M}(P')$. We also consider sometimes minimal proof P for $|P|$ instead of $\mathcal{M}(P)$.

Lastly we say that a proof P is a successive sequence of applications of decomposition rule on the i-th element of Φ when there exists $n \in \mathbb{N}$ such that $P = \mathsf{ir}_n(\ldots ir_1(i, P_1, \ldots, P_m) \ldots, P'_1, \ldots, P'_{m'})$ and each ir_k is a decomposition rule for $k = 1 \ldots n$.

We denote by $st_<(t)$ the set of strict subterms of t. We naturally extend this notion to frames.

▶ **Lemma 19.** *Let Φ be a frame. Let $t \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathcal{X})$ such that $\Phi \vdash t$. For all P minimal proofs for $|P|$ of $\Phi \vdash t$, for all $P' \in st(P)$, for all terms t', if $\Phi \vdash_{P'} t'$ then*

- *$\mathsf{root}(t') \notin \mathcal{F}_{key}$ and $\mathsf{root}(P)$ is a composition rule imply $t' \in st(\Phi) \cup st(t)$;*

- $\mathsf{root}(t') \notin \mathcal{F}_{key}$ *and* $\mathsf{root}(P)$ *is a decomposition rule imply* $t' \in st(\Phi)$*;*
- $t' = \mathsf{f}(u)$ *for some term* u *and* $\mathsf{f} \in \mathcal{F}_{key}$ *implies* $u \in st_<(\Phi) \cup st_<(t)$.

Proof. We show the result by induction on $\mathcal{M}(P)$.

Base case $|P| = 1$*:* In such a case, $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. In the former, $\mathsf{root}(t) \notin \mathcal{F}_{key}$ and $\mathsf{root}(P)$ is neither a composition rule nor a decomposition rule. Hence the result directly holds. In the latter, $t \in \Phi$ and $\mathsf{root}(P)$ is neither a composition rule nor a decomposition rule. Therefore, if $t = \mathsf{f}(u)$ for some term u and $\mathsf{f} \in \mathcal{F}_{key}$ then we directly have that $u \in st_<(\Phi)$. Hence the result holds.

Induction case $|P| > 1$*:* Otherwise $\mathsf{root}(P)$ is an inference rule. Therefore, we have :

$$\frac{t_1 \quad \dots \quad t_n}{t}$$

with $P = \mathsf{ir}(P_1, \dots, P_n)$ and for all $k \in \{1, \dots, n\}$, $\Phi \vdash_{P_k} t_k$. Applying the inductive hypothesis we can deduce that for all $k \in \{1, \dots, n\}$, for all $P' \in st(P_k)$, for all t', if $\Phi \vdash_{P'} t'$ then :

- $\mathsf{root}(t') \notin \mathcal{F}_{key}$ and $\mathsf{root}(P_k)$ is a composition rule imply $t' \in st(\Phi) \cup st(t_k)$;
- $\mathsf{root}(t') \notin \mathcal{F}_{key}$ and $\mathsf{root}(P_k)$ is a decomposition rule imply $t' \in st(\Phi)$;
- $t' = \mathsf{f}(u)$ for some term u and $\mathsf{f} \in \mathcal{F}_{key}$ implies $u \in st_<(\Phi) \cup st_<(t_k)$.

Let $P' \in st(P)$ and let t' be a term such that $\Phi \vdash_{P'} t'$. Let us do a case analysis on whether ir is a decomposition or a composition rule.

- Case ir is a composition rule: In such a case, there exists a function symbol f such that $t = \mathsf{f}(t_1, \dots, t_n)$, implying that for all $k \in \{1, \dots, n\}$, $st(\Phi) \cup st(t_k) \subseteq st(\Phi) \cup st(t)$ and $st_<(\Phi) \cup st_<(t_k) \subseteq st_<(\Phi) \cup st_<(t)$. Hence, if $P' \in st(P_k)$ for some $k \in \{1, \dots, n\}$ the result directly holds given our inductive hypothesis. Consider now $P' = P$ and so $t' = t$. In such a case, if $\mathsf{root}(t) \notin \mathcal{F}_{key}$ then we directly have that $t \in st(t)$ else $t = \mathsf{f}(u)$ with $\mathsf{f} \in \mathcal{F}_{key}$ and $u \in st_<(t)$. Therefore the result holds.
- Case ir is a decomposition rule: Otherwise $t_1 = \mathsf{f}(t, u_1, \dots, u_m)$ for some term $u_1, \dots, u_m$ and $\mathsf{f} \notin \mathcal{F}_{key}$. Since P is minimal, we deduce that either $\mathsf{root}(P_1)$ is a decomposition rule or $P = t_1$ meaning that $t_1 \in \Phi$ (otherwise there would exist $P'_1 \in st(P_1)$ such that $\Phi \vdash_{P'_1} t$ and $|P'_1| < |P|$). Let us first focus on $P' \in st(P_1)$. If $\mathsf{root}(t') \notin \mathcal{F}_{key}$ then by our inductive hypothesis and knowing that ir is a decomposition rule, we obtain that $t' \in st(\Phi)$. In particular when $P' = P_1$ we deduce that $\mathsf{f}(t, u_1, \dots, u_m) \in st(\Phi)$. Moreover, if $t' = \mathsf{g}(u)$ with $\mathsf{g} \in \mathcal{F}_{key}$ then $u \in st_<(\Phi) \cup st_<(\mathsf{f}(t, u_1, \dots, u_m))$. Since $\mathsf{f}(t, u_1, \dots, u_m) \in st(\Phi)$, $u \in st_<(\mathsf{f}(t, u_1, \dots, u_m))$ implies $u \in st_<(\Phi)$. Hence the result holds.
  Note that $\mathsf{f}(t, u_1, \dots, u_m) \in st(\Phi)$ allows us to directly prove that $t \in st(\Phi)$ hence the result holds in the case $P' = P$ and $t' = t$.
  Let us now focus on the case where $P' \in st(P_k)$ for some $k \in \{2, \dots, n\}$. By our inductive hypothesis, we know that $\mathsf{root}(t') \notin \mathcal{F}_{key}$ implies $t' \in st(\Phi) \cup st(t_k)$. But from the definition of a decomposition rule, we know that for all $k \in \{2, \dots, n\}$, either $t_k \in st_<(\mathsf{f}(t, u_1, \dots, u_m))$ or $\mathsf{root}(t_k) \in \mathcal{F}_{key}$ and $st_<(t_k) \subseteq st_<(\mathsf{f}(t, u_1, \dots, u_m))$. In the former, since $\mathsf{f}(t, u_1, \dots, u_m) \in st(\Phi)$ then we directly deduce that $t' \in st(\Phi)$. In the latter, since $\mathsf{root}(t') \notin \mathcal{F}_{key}$ and $\mathsf{root}(t_k) \in \mathcal{F}_{key}$ then $t' \in st(t_k)$ implies $t' \in st_<(t_k)$ and so $t' \in st_<(\mathsf{f}(t, u_1, \dots, u_m)) \subseteq st(\Phi)$.
  If $t' = \mathsf{g}(u)$ with $\mathsf{g} \in \mathcal{F}_{key}$ then by our inductive hypothesis, $u \in st_<(\Phi) \cup st_<(t_k)$. But we have already shown that $st_<(t_k) \subseteq st_<(\mathsf{f}(t, u_1, \dots, u_m))$ and $\mathsf{f}(t, u_1, \dots, u_m) \in st(\Phi)$. Hence we deduce that $u \in st_<(t_k)$ implies that $u \in st_<(\Phi)$ which allows us to conclude.

◂

B.1 BAC encapsulation

▶ **Lemma 20.** *Let* $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \in \mathsf{Tag}$. *Let* $\mathcal{E}_{\mathsf{BAC}} = \langle t, h(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \langle t, z\rangle\rangle)\rangle$ *with* $t = \mathsf{senc}(\langle \mathsf{a}, x\rangle, y)$, $\mathsf{t}_{\mathcal{E}_{\mathsf{BAC}}} = x$ *and* $\mathsf{X}_{\mathcal{E}_{\mathsf{BAC}}} = (y, z)$. *We have that* $(\mathcal{E}_{\mathsf{BAC}}, \emptyset)$ *is a* $\{\mathsf{a}_{\mathcal{E}\mathsf{BAC}}\}$*-tagged encapsulation and* $\mathcal{S} = \{(\mathcal{E}_{\mathsf{BAC}}, \emptyset)\}$ *allows secure channels.*

Proof. Let $(\mathcal{E}_1, \emptyset), \ldots, (\mathcal{E}_n, \emptyset) \in \mathcal{S}$ such that the variables of $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are disjoints. Since $\mathcal{S} = \{(\mathcal{E}_{\mathsf{BAC}}, \emptyset)\}$, we have that $\mathcal{E}_i \sim \mathcal{E}_j$ for all $i, j \in \{1, \ldots, n\}$. For all $i \in \{1, \ldots, n\}$, we will denote $\mathsf{t}_{\mathcal{E}_i} = x_i$ and $\mathsf{X}_{\mathcal{E}_i} = (y_i, z_i)$. Let σ be a ground substitution such that $dom(\sigma) \subseteq vars(\mathcal{E}_1, \ldots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(\sigma, \Phi)$. Finally, let $I = \{i \in \{1, \ldots, n\} \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma\}$. We show that for all $i \in \{1, \ldots, n\}$, Properties 1, 2, 4 and 6 of Definition 7 hold.

Property 1: Let $i \in \{1, \ldots, n\}$. Let $t \in \mathcal{T}(\mathcal{F}_{key}, \{y_i\sigma, z_i\sigma\})$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P t$. Assume that P is minimal for $|P|$. We do a case analysis on $|P|$. If $|P| = 1$ then either $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$ or $t = \mathcal{E}_k\sigma$ for some $k \in \{1, \ldots, n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(t)$. Hence, we deduce that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. Therefore, $\Phi \vdash t$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$.

Otherwise, $|P| > 1$. Let us assume that there exist $j \in \{1, \ldots, n\}$ and $P' \in st(P)$ such that $P' = |\Phi| + j$. Since $|P| > 1$, we deduce that there exist $\mathsf{ir}, P'', P_1, \ldots, P_m, \ell \in \{1, \ldots, m\}$ such that $P'' = \mathsf{ir}(P_1, \ldots, P_m) \in st(P)$ and $P_\ell = P'$. Let us denote t'' the term $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} t''$. By Lemma 19, we deduce that either $t'' \in st(\Phi) \cup st(\mathcal{E}_k\sigma)_{k=1}^n \cup st(t)$ or $t'' = \mathsf{g}(u)$ for some $\mathsf{g} \in \mathcal{F}_{key}$ and $u \in st_<(\Phi) \cup st_<(\mathcal{E}_k\sigma)_{k=1}^n \cup st_<(t)$. Since $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(t, \sigma, \Phi)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} \mathcal{E}_j\sigma$ and all $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are equal after variable renaming, we deduce that in both cases, ir cannot be a composition rule. Since ir is a decomposition rule, we in fact have $P'' = \mathsf{ir}(P')$ where ir is one of the pair decomposition. Moreover, either $t'' = \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \langle u, z_i\sigma\rangle\rangle)$ where $u = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_i\sigma\rangle, y_i\sigma)$ or $t'' = u$. Once again since $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(t)$, we deduce that $P'' \neq P$. Thus, there exists $Q = \mathsf{ir}'(Q_1, \ldots, Q_\ell)$ and $\ell' \in \{1, \ldots, \ell\}$ such that $Q \in st(P)$ and $Q_{\ell'} = P''$.

By the Lemma 19, we can easily show that ir' cannot be a composition rule for some $\mathsf{g} \notin \mathcal{F}_{key}$ since if would imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathcal{E}_r\sigma$ for some r which would contradict our hypothesis on the minimality of $|P|$. We also show that ir' cannot be is a composition rule for some $\mathsf{g} \in \mathcal{F}_{key}$. In such a case, it would imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathsf{g}(t'')$. But since $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \in st(t'')$, then $Q \neq P$ and so there must be another inference rule ir'' applied on Q in P. Once again, by Lemma 19, ir'' cannot be a composition rule for any function symbol since it would imply that $\mathsf{g}(t'') \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n) \cup st(t)$ but $\mathcal{E}_{\mathsf{BAC}}$ does not contain function symbol from $\mathcal{F}_{key}$ and $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(t, \sigma, \Phi)$. Moreover, ir'' cannot be a decomposition rule either since the only rule involving a function symbol $\mathsf{g} \in \mathcal{F}_{key}$ as argument is the signature decomposition which would imply that there exists a term v and a proof $R \in st(P)$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_R \mathsf{sign}(v, t'')$. Once again, this is prevented by Lemma 19. Therefore, we can conclude that ir' cannot be a composition rule for some $\mathsf{g} \in \mathcal{F}_{key}$.

Thus, ir' is a decomposition rule. Note that once again thanks to Lemma 19 and the fact that $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(t, \sigma, \Phi)$, we can deduce that $j' = 1$ meaning that t'' is not used as a key in the decomposition rule ir'. But there is no decomposition rule for h, thus $t'' = \mathsf{senc}(\langle \mathsf{a}, x_j\sigma\rangle, y_j\sigma)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{Q_2} y_j\sigma$. This allows us to deduce that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_j\sigma\rangle$. But $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_j\sigma\rangle$ also imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_j\sigma$ and so $j \in I$. Therefore, $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_j\sigma\rangle$.

We have just shown that for all $j \in \{1, \ldots, n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j and a term u such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} u$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{Q_j} u$. Therefore, by replacing all instances of $P|_{p'_j}$ in P by Q_j, we obtain that a proof P' such that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{P'} t$. This allows us to conclude.

Property 2: Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and $v \in st(\mathcal{E}_j) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\rangle$. By definition of $\mathcal{E}_{\mathsf{BAC}}$, u, v unifiable implies that there exists a position p of $\mathcal{E}_{\mathsf{BAC}}$ such that $u = \mathcal{E}_i|_p$ and $v = \mathcal{E}_j|_p$. Since $\mathcal{E}_i \sim \mathcal{E}_j$ then the result holds.

Property 4: Let $i \in \{1,\dots,n\}$. Consider a minimal proof P for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P x_i\sigma$. We do a case analysis on $|P|$. If $|P| = 1$ then either $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$ or $x_i\sigma = \mathcal{E}_k\sigma$ for some $k \in \{1,\dots,n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(x_i\sigma)$. Hence, we deduce that $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$. Therefore, $\Phi \vdash x_i\sigma$ and so $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_i\sigma$.

Otherwise, $|P| > 1$. Following exactly the proof of Property 1 (replacing t by $x_i\sigma$), we deduce that for all $j \in \{1,\dots,n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j such that $P|_{p'_j} = \mathsf{ir}_1(\mathsf{ir}_2(|\Phi|+j), Q_j)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} \langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_j\sigma\rangle$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{Q_j} y_j\sigma$ where ir_1 is the decomposition rule of senc and ir_2 is the first decomposition rule of $\langle\,\rangle$. Let us look at the proof Q_j. Since $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(y_j\sigma)$, we can deduce by minimality of $|P|$ that $|\Phi|+j \notin Q_j$ (otherwise, using the same reasoning, it would imply that there exists a proof $Q'_j \in st_<(Q_j)$ deducing $y_i\sigma$). Thus, $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash_{Q_j} y_j\sigma$. Let $I' = \{i \in \{1,\dots,n\} - j \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash x_i\sigma\}$. Note that $I' \subseteq I - j$. By applying Property 1 on $y_j\sigma$ with $[\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j}$ and I', we deduce that $\Phi \cdot [x_k\sigma]_{k\in I'} \vdash y_j\sigma$.

Therefore, we have proven that if $|\Phi| + i \in st(P)$ then $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash y_j\sigma$. Otherwise, if for all $j \in \{1,\dots,n\}$, for all position p_j of P, $P|_{p_j} = |\Phi| + j$ implies that $i \neq j$ then we also have proven that $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_j\sigma$ using the same replacement of proofs as in the proof of Property 1. Hence, the result holds.

Property 6: Let $i \in \{1,\dots,n\}$. Let σ' some ground substitution such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$ and $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(\sigma')$, if we denote $J = I - i$ then. Consider a proof P minimal for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P \mathcal{E}_i\sigma'$. If $|P| = 1$ then it implies that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}$ due to the fact that $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(\Phi)$. Therefore, there exists $k \in \{1,\dots,n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$. Since we already know that $\mathcal{E}_i \sim \mathcal{E}_k$ then the result holds.

Otherwise $|P| > 1$. In such a case $P = \mathsf{ir}(P_1,\dots,P_n)$. We do a case analysis on ir.

- Case ir is a decomposition rule: By Lemma 19, we deduce that $\mathcal{E}_i\sigma' \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n)$. But since $\mathsf{a}_{\mathcal{E}\mathsf{BAC}} \notin st(\Phi) \cup st(\sigma)$, then we deduce that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}^n$ which contradicts the minimality of $|P|$.
- Case ir is a composition rule: In such a case, we have $P = \mathsf{ir}(P_1, P_2)$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_1} u$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_2} \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \langle u, z_i\sigma'\rangle\rangle)$ with $u = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_i\sigma'\rangle, y_i\sigma')$. Let us first focus on P_2. If the last rule of P_2 starts by a decomposition rule, then by Lemma 19, we deduce that $\mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \langle u, z_i\sigma'\rangle\rangle) \in st([\mathcal{E}_k\sigma]_{k=1}^n)$ which would then imply that there exists $k \in \{1,\dots,n\}$ such that $\mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \langle u, z_i\sigma'\rangle\rangle) = \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \langle v, z_k\sigma\rangle\rangle)$ with $v = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_k\sigma\rangle, y_k\sigma)$. Therefore, $x_k\sigma = x_i\sigma'$ and so $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$ which contradicts our hypothesis on the minimality of $|P|$. Therefore, the last rule of P_2 is necessarily a composition rule, implying that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash z_i\sigma'$. Following the same proof of Property 1 (replacing t by $z_i\sigma'$), we deduce that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash z_i\sigma'$.
  Let us now consider P_1. If P_1 starts by a decomposition rule, then by Lemma 19, we deduce that $\mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x_i\sigma'\rangle, y_i\sigma') \in st([\mathcal{E}_k\sigma]_{k=1}^n)$. Thus, it implies that there exists $j \in \{1,\dots,n\}$ such that $x_i\sigma' = x_j\sigma$ and $y_i\sigma' = y_j\sigma$ meaning that $\mathsf{X}_{\mathcal{E}_i}\sigma' \cap \mathsf{X}_{\mathcal{E}_j}\sigma \neq \emptyset$. Hence the result holds. If on the other hand, P_1 starts by a composition rule then we directly have that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma'$. Once again by following the same proof as in Property 1 (replacing t by $x_i\sigma'$), we deduce that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash x_i\sigma'$.

◀

B.2 TLS encapsulation

▶ **Lemma 21.** *Let* $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \in \mathsf{Tag}$. *Let* $\mathcal{E}_{\mathsf{TLS}} = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x\rangle, y)$, $\mathsf{t}_{\mathcal{E}_{\mathsf{TLS}}} = x$ *and* $\mathsf{X}_{\mathcal{E}_{\mathsf{TLS}}} = y$. *We have that* $(\mathcal{E}_{\mathsf{TLS}}, \emptyset)$ *is a* $\{\mathsf{a}_{\mathcal{E}\mathsf{TLS}}\}$*-tagged encapsulation and* $\mathcal{S} = \{(\mathcal{E}_{\mathsf{TLS}}, \emptyset)\}$ *allows secure channels.*

Proof. Let $(\mathcal{E}_1, \emptyset), \dots, (\mathcal{E}_n, \emptyset) \in \mathcal{S}$ such that the variables of $\mathcal{E}_1, \dots, \mathcal{E}_n$ are disjoints. Since $\mathcal{S} = \{(\mathcal{E}_{\mathsf{TLS}}, \emptyset)\}$, we have that $\mathcal{E}_i \sim \mathcal{E}_j$ for all $i, j \in \{1,\dots,n\}$. For all $i \in \{1,\dots,n\}$, we will denote $\mathsf{t}_{\mathcal{E}_i} = x_i$

and $\mathsf{X}_{\mathcal{E}_i} = y_i$. Let σ be a ground substitution such that $dom(\sigma) \subseteq vars(\mathcal{E}_1, \ldots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(\sigma, \Phi)$. Finally, let $I = \{i \in \{1, \ldots, n\} \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma\}$. We show that for all $i \in \{1, \ldots, n\}$, Properties 1, 2, 4 and 6 of Definition 7 hold.

Property 1: Let $i \in \{1, \ldots, n\}$. Let $t \in \mathcal{T}(\mathcal{F}_{key}, \{y_i\sigma\})$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P t$. Assume that P is minimal for $|P|$. We do a case analysis on $|P|$. If $|P| = 1$ then either $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$ or $t = \mathcal{E}_k\sigma$ for some $k \in \{1, \ldots, n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(t)$. Hence, we deduce that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. Therefore, $\Phi \vdash t$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$.

Otherwise, $|P| > 1$. Let us assume that there exists $j \in \{1, \ldots, n\}$ and $P' \in st(P)$ such that $P' = |\Phi| + j$. Since $|P| > 1$, we deduce that there exists ir, $P'', P_1, \ldots, P_m$, $\ell \in \{1, \ldots, m\}$ such that $P'' = \mathsf{ir}(P_1, \ldots, P_m) \in st(P)$ and $P_\ell = P'$. Let us denote t'' the term $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} t''$. By Lemma 19, we deduce that either $t'' \in st(\Phi) \cup st(\mathcal{E}_k\sigma)_{k=1}^n \cup st(t)$ or $t'' = \mathsf{g}(u)$ for some $\mathsf{g} \in \mathcal{F}_{key}$ and $u \in st_<(\Phi) \cup st_<(\mathcal{E}_k\sigma)_{k=1}^n \cup st_<(t)$. Since $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(t, \sigma, \Phi)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} \mathcal{E}_j\sigma$ and all $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are equal after variable renaming, we deduce that in both cases, ir cannot be a composition rule. Since ir is a decomposition rule, we in fact have $P'' = \mathsf{ir}(P', Q)$ where ir is the senc decomposition and $t'' = \langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x_j\sigma \rangle$. Thus we have that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} x_j\sigma$ and so $j \in I$. Therefore, $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x_j\sigma \rangle$.

We have just shown that for all $j \in \{1, \ldots, n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j and a term u such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} u$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{Q_j} u$. Therefore, by replacing all instances of $P|_{p'_j}$ in P by Q_j, we obtain that a proof P' such that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{P'} t$. This allows us to conclude.

Property 2: Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and $v \in st(\mathcal{E}_j) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\rangle$. By definition of $\mathcal{E}_{\mathsf{TLS}}$, u, v unifiable implies that there exists a position p of $\mathcal{E}_{\mathsf{TLS}}$ such that $u = \mathcal{E}_i|_p$ and $v = \mathcal{E}_j|_p$. Since $\mathcal{E}_i \sim \mathcal{E}_j$ then the result holds.

Property 4: Let $i \in \{1, \ldots, n\}$. Consider a minimal proof P for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P x_i\sigma$. We do a case analysis on $|P|$. If $|P| = 1$ then either $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$ or $x_i\sigma = \mathcal{E}_k\sigma$ for some $k \in \{1, \ldots, n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(x_i\sigma)$. Hence, we deduce that $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$. Therefore, $\Phi \vdash x_i\sigma$ and so $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_i\sigma$.

Otherwise, $|P| > 1$. Following exactly the proof of Property 1 (replacing t by $x_i\sigma$), we deduce that for all $j \in \{1, \ldots, n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j such that $P|_{p'_j} = \mathsf{ir}(|\Phi| + j, Q_j)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} \langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x_j\sigma \rangle$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{Q_j} y_j\sigma$ where ir is the decomposition rule of senc. Let us look at the proof Q_j. Since $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(y_j\sigma)$, we can deduce by minimality of $|P|$ that $|\Phi| + j \notin Q_j$ (otherwise, using the same reasoning, it would imply that there exists a proof $Q'_j \in st_<(Q_j)$ deducing $y_i\sigma$). Thus, $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\ldots,n\}-j} \vdash_{Q_j} y_j\sigma$. Let $I' = \{i \in \{1, \ldots, n\} - j \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\ldots,n\}-j} \vdash x_i\sigma\}$. Note that $I' \subseteq I - j$. By applying Property 1 on $y_j\sigma$ with $[\mathcal{E}_k\sigma]_{k\in\{1,\ldots,n\}-j}$ and I', we deduce that $\Phi \cdot [x_k\sigma]_{k\in I'} \vdash y_j\sigma$.

Therefore, we have proven that if $|\Phi| + i \in st(P)$ then $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash y_i\sigma$. Otherwise, if for all $j \in \{1, \ldots, n\}$, for all position p_j of P, $P|_{p_j} = |\Phi| + j$ implies that $i \neq j$ then we also have proven that $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_j\sigma$ using the same replacement of proofs as in the proof of Property 1. Hence, the result holds.

Property 6: Let $i \in \{1, \ldots, n\}$. Let σ' be some ground substitution such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$. Consider a proof P minimal for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P \mathcal{E}_i\sigma'$. If $|P| = 1$ then it implies that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}$ due to the fact that $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(\Phi)$. Therefore, there exists $k \in \{1, \ldots, n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$. Since we already know that $\mathcal{E}_i \sim \mathcal{E}_k$ then the result holds.

Otherwise $|P| > 1$. In such a case $P = \mathsf{ir}(P_1, \ldots, P_n)$. We do a case analysis on ir.

- Case ir is a decomposition rule: by Lemma 19, we deduce that $\mathcal{E}_i\sigma' \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n)$. But since $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(\Phi) \cup st(\sigma)$, then we deduce that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}^n$ which contradicts the minimality of $|P|$.

- Case ir is a composition rule: Then we directly have that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma'$. Once again by following the same proof as in Property 1 (replacing t by $x_i\sigma'$), we deduce that $\Phi\cdot[\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash x_i\sigma'$.

◀

B.3 Signcrypt encapsulation

▶ **Lemma 22.** *Let* $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \in \mathsf{Tag}$. *Let* $\mathcal{E}_{\mathsf{signcrypt}} = \mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x\rangle, \mathsf{pk}(y))\rangle, z)$ *with* $\mathsf{t}_{\mathcal{E}_{\mathsf{signcrypt}}} = x$ *and* $\mathsf{X}_{\mathcal{E}_{\mathsf{signcrypt}}} = (y, z)$. *We have that* $(\mathcal{E}_{\mathsf{signcrypt}}, \emptyset)$ *is a* $\{\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}\}$*-tagged encapsulation and* $\mathcal{S} = \{(\mathcal{E}_{\mathsf{signcrypt}}, \emptyset)\}$ *allows secure channels.*

Proof. Let $(\mathcal{E}_1, \emptyset), \ldots, (\mathcal{E}_n, \emptyset) \in \mathcal{S}$ such that the variables of $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are disjoints. Since $\mathcal{S} = \{(\mathcal{E}_{\mathsf{signcrypt}}, \emptyset)\}$, we have that $\mathcal{E}_i \sim \mathcal{E}_j$ for all $i, j \in \{1, \ldots, n\}$. For all $i \in \{1, \ldots, n\}$, we will denote $\mathsf{t}_{\mathcal{E}_i} = x_i$ and $\mathsf{X}_{\mathcal{E}_i} = (y_i, z_i)$. Let σ be a ground substitution such that $dom(\sigma) \subseteq vars(\mathcal{E}_1, \ldots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(\sigma, \Phi)$. Finally, let $I = \{i \in \{1, \ldots, n\} \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma\}$. We show that for all $i \in \{1, \ldots, n\}$, Properties 1, 2, 4 and 6 of Definition 7 hold.

We first prove that for all term t such that $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(t)$, $\Phi\cdot[\mathcal{E}_k\sigma]_{k=1}^n \vdash_P t$ implies $\Phi\cdot[x_k\sigma]_{k\in I} \vdash t$. Assume that P is minimal for $|P|$. We do a case analysis on $|P|$. If $|P| = 1$ then either $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$ or $t = \mathcal{E}_k\sigma$ for some $k \in \{1, \ldots, n\}$. But $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(t)$. Hence, we deduce that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. Therefore, $\Phi \vdash t$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$.

Otherwise, $|P| > 1$. Let us assume that there exist $j \in \{1, \ldots, n\}$ and $P' \in st(P)$ such that $P' = |\Phi| + j$. Since $|P| > 1$, we deduce that there exist ir, $P'', P_1, \ldots, P_m$, $\ell \in \{1, \ldots, m\}$ such that $P'' = \mathsf{ir}(P_1, \ldots, P_m) \in st(P)$ and $P_\ell = P'$. Let us denote t'' the term $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} t''$. By Lemma 19, we deduce that either $t'' \in st(\Phi) \cup st(\mathcal{E}_k\sigma)_{k=1}^n \cup st(t)$ or $t'' = \mathsf{g}(u)$ for some $\mathsf{g} \in \mathcal{F}_{key}$ and $u \in st_<(\Phi) \cup st_<(\mathcal{E}_k\sigma)_{k=1}^n \cup st_<(t)$. Since $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(t, \sigma, \Phi)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} \mathcal{E}_j\sigma$ and all $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are equal after variable renaming, we deduce that in both cases, ir cannot be a composition rule. Since ir is a decomposition rule, we in fact have $P'' = \mathsf{ir}(P', R)$ where ir the rule sign-decomp and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_R \mathsf{vk}(z_j\sigma)$. Moreover, we have $t'' = \langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_j\sigma\rangle, \mathsf{pk}(y_j\sigma))\rangle$. Once again since $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(t)$, we deduce that $P'' \neq P$. Thus, there exists $Q = \mathsf{ir}'(Q_1, \ldots, Q_\ell)$ and $\ell' \in \{1, \ldots, \ell\}$ such that $Q \in st(P)$ and $Q_{\ell'} = P''$.

By the Lemma 19, we can easily show that ir' cannot be a composition rule for some $\mathsf{g} \notin \mathcal{F}_{key}$ since if would imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathcal{E}_r\sigma$ for some r which would contradict our hypothesis on the minimality of $|P|$. We also show that ir' cannot be is a composition rule for some $\mathsf{g} \in \mathcal{F}_{key}$. In such a case, it would imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathsf{g}(t'')$. But since $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \in st(t'')$, then $Q \neq P$ and so there must be another inference rule ir'' applied on Q in P. Once again, by Lemma 19, ir'' cannot be a composition rule for any function symbol since it would imply that $\mathsf{g}(t'') \in st(\Phi)\cup st([\mathcal{E}_k\sigma]_{k=1}^n)\cup st(t)$ but $\mathcal{E}_{\mathsf{signcrypt}}$ only contain the function symbol pk applied on y. But since $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(\sigma)$, we deduce that $\mathsf{pk}(y_k)\sigma \neq \mathsf{g}(t'')$ for all k. Moreover, ir'' cannot be a decomposition rule either since the only rule involving a function symbol $\mathsf{g} \in \mathcal{F}_{key}$ as argument is the signature decomposition which would imply that there exists a term v and a proof $R \in st(P)$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_R \mathsf{sign}(v, t'')$. Once again, this is prevented by Lemma 19 since $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(\sigma)$. Therefore, we can conclude that ir' cannot be a composition rule for some $\mathsf{g} \in \mathcal{F}_{key}$.

Thus ir' is a decomposition rule and in fact the second decomposition of the pairing implying that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_j\sigma\rangle, \mathsf{pk}(y_j\sigma))$. Using a similar reasoning as above, we can prove that there exists $R = \mathsf{ir}''(R_1, \ldots, R_p)$ and $p' \in \{1, \ldots, p\}$ such that $R \in st(P)$ and $R_{p'} = Q$. Moreover, by Lemma 19, ir'' cannot be a f-composition for $\mathsf{f} \notin \mathcal{F}_{key}$ since the only function f possible would be the pair but it would contradict our minimality hypothesis. Similarly as above, we can also prove that ir' cannot be f-composition for $\mathsf{f} \in \mathcal{F}_{key}$. Therefore, it remains that ir'' is a decomposition rule meaning that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_R \langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_j\sigma\rangle$. But it also implies that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_j\sigma$ meaning that $j \in I$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_j\sigma\rangle$.

We have just shown that for all $j \in \{1,\dots,n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j and a term u such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} u$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{Q_j} u$. Therefore, by replacing all instances of $P|_{p'_j}$ in P by Q_j, we obtain that a proof P' such that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{P'} t$. This allows us to conclude.

Property 1: For all $i \in \{1,\dots,n\}$, for all $t \in \mathcal{T}(\mathcal{F}_{key}, \{y_i\sigma, z_i\sigma\})$, we have that $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(t)$. Hence we can apply the property we just proved which allows us to conclude.

Property 2: Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and $v \in st(\mathcal{E}_j) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\rangle$. By definition of $\mathcal{E}_{\mathsf{signcrypt}}$, u, v unifiable implies that there exists a position p of $\mathcal{E}_{\mathsf{signcrypt}}$ such that $u = \mathcal{E}_i|_p$ and $v = \mathcal{E}_j|_p$. Since $\mathcal{E}_i \sim \mathcal{E}_j$ then the result holds.

Property 4: Let $i \in \{1,\dots,n\}$. Consider a minimal proof P for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P x_i\sigma$. We do a case analysis on $|P|$. If $|P| = 1$ then either $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$ or $x_i\sigma = \mathcal{E}_k\sigma$ for some $k \in \{1,\dots,n\}$. But $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(x_i\sigma)$. Hence, we deduce that $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$. Therefore, $\Phi \vdash x_i\sigma$ and so $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_i\sigma$.

Otherwise, $|P| > 1$. Following exactly the proof of the property we prove at the beginning of this lemma, we deduce that for all $j \in \{1,\dots,n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j such that $P|_{p'_j} = \mathsf{ir}_1(\mathsf{ir}_2(\mathsf{ir}_3(|\Phi| + j, Q_j)), R_j)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} \langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_j\sigma\rangle$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{Q_j} \mathsf{vk}(z_j\sigma)$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{R_j} y_j\sigma$ where ir_1 is the decomposition rule of aenc, ir_2 is the second decomposition rule of $\langle\ \rangle$ and ir_3 is the decomposition of sign. Let us look at the proofs Q_j and R_j. Since $\mathsf{a}_{\mathcal{E}_{\mathsf{BAC}}} \notin st(y_j\sigma, z_j\sigma)$, we can deduce by minimality of $|P|$ that $|\Phi| + j \notin Q_j$ and $|\Phi| + j \notin R_j$ (otherwise, using the same reasoning, it would imply that there exists a proof $Q'_j \in st_<(Q_j)$ (resp. R'_j) deducing $\mathsf{vk}(z_j\sigma)$ (resp. $y_j\sigma$)). Thus, $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash_{Q_j} \mathsf{vk}(z_j\sigma)$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash_{R_j} y_j\sigma$. Let $I' = \{i \in \{1,\dots,n\} - j \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash x_i\sigma\}$. Note that $I' \subseteq I - j$. By applying Property 1 on $y_j\sigma$ and $\mathsf{vk}(z_j\sigma)$ with $[\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j}$ and I', we deduce that $\Phi \cdot [x_k\sigma]_{k\in I'} \vdash y_j\sigma$ and $\Phi \cdot [x_k\sigma]_{k\in I'} \vdash \mathsf{vk}(z_j\sigma)$.

Therefore, we have proven that if $|\Phi|+i \in st(P)$ then $\Phi\cdot[x_k\sigma]_{k\in I-i} \vdash y_i\sigma$ which satisfies Property 4. Otherwise, if for all $j \in \{1,\dots,n\}$, for all position p_j of P, $P|_{p_j} = |\Phi| + j$ implies that $i \neq j$ then we also have proven that $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_j\sigma$ by the first property proven in this lemma.

Property 6: Let $i \in \{1,\dots,n\}$. Let σ' some ground substitution such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$. Consider a proof P minimal for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P \mathcal{E}_i\sigma'$. If $|P| = 1$ then it implies that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}$ due to the fact that $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(\Phi)$. Therefore, there exists $k \in \{1,\dots,n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$. Since we already know that $\mathcal{E}_i \sim \mathcal{E}_k$ then the result holds.

Otherwise $|P| > 1$. In such a case $P = \mathsf{ir}(P_1,\dots,P_n)$. We do a case analysis on ir.

- Case ir is a decomposition rule: By Lemma 19, we deduce that $\mathcal{E}_i\sigma' \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n)$. But since $\mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}} \notin st(\Phi) \cup st(\sigma)$, then we deduce that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}^n$ which contradicts the minimality of $|P|$.
- Case ir is a composition rule: In such a case, we have $P = \mathsf{ir}(P_1, P_2)$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_1} \langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_i\sigma'\rangle, \mathsf{pk}(y_i\sigma'))\rangle$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_2} z_i\sigma'$. The latter already gives us part of Property thanks to the first property of the lemma. Let us now focus on P_1.
  If the last rule of P_1 starts by a decomposition rule, then by Lemma 19, we deduce that $\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_i\sigma'\rangle, \mathsf{pk}(y_i\sigma'))\rangle \in st([\mathcal{E}_k\sigma]_{k=1}^n)$ which would then imply that there exists $k \in \{1,\dots,n\}$ such that $x_i\sigma' = x_k\sigma$ and $y_i\sigma' = y_k\sigma$. Therefore the result holds. If the last rule of P_2 is a composition then we have $P_1 = \mathsf{ir}'(Q_1, Q_2)$ where $\Phi\cdot[\mathcal{E}_k\sigma]_{k=1}^n \vdash_{Q_2} \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_i\sigma'\rangle, \mathsf{pk}(y_i\sigma'))$. If the last rule of Q_2 is a composition rule then it would imply that $\Phi\cdot[\mathcal{E}_k\sigma]_{k=1}^n \vdash \langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_i\sigma'\rangle$ and so $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma'$ which would allow us to conclude. If on the other hand the last rule of Q_2 is a decomposition rule, then once again we would deduce that $\mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}_{\mathsf{signcrypt}}}, x_i\sigma'\rangle, \mathsf{pk}(y_i\sigma')) \in$

$st([\mathcal{E}_k\sigma]_{k=1}^n)$ and so there would exists $k \in \{1,\dots,n\}$ such that $x_i\sigma' = x_k\sigma$ and $y_i\sigma' = y_k\sigma$. This allows us to conclude.

◂

B.4 Sign encapsulation

▸ **Lemma 23.** *Let* $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \in \mathsf{Tag}$. *Let* $\mathcal{E}_{\mathsf{sign}} = \mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x\rangle, y)$ *with* $\mathsf{t}_{\mathcal{E}_{\mathsf{signcrypt}}} = x$ *and* $\mathsf{X}_{\mathcal{E}_{\mathsf{sign}}} = y$. *We have that* $(\mathcal{E}_{\mathsf{sign}}, \mathsf{vk}(y))$ *is a* $\{\mathsf{a}_{\mathcal{E}\mathsf{sign}}\}$*-tagged encapsulation and* $\mathcal{S} = \{(\mathcal{E}_{\mathsf{sign}}, \mathsf{vk}(y))\}$ *allows authentic channels.*

Proof. Let $(\mathcal{E}_1, \emptyset), \dots, (\mathcal{E}_n, \emptyset) \in \mathcal{S}$ such that the variables of $\mathcal{E}_1, \dots, \mathcal{E}_n$ are disjoints. Since $\mathcal{S} = \{(\mathcal{E}_{\mathsf{signcrypt}}, \mathsf{vk}(y))\}$, we have that $\mathcal{E}_i \sim \mathcal{E}_j$ for all $i, j \in \{1,\dots,n\}$. For all $i \in \{1,\dots,n\}$, we will denote $\mathsf{t}_{\mathcal{E}_i} = x$ and $\mathsf{X}_{\mathcal{E}} = y_i$. Let σ be a ground substitution such that $dom(\sigma) \subseteq vars(\mathcal{E}_1, \dots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{a}_{\mathcal{E}\mathsf{signcrypt}} \notin st(\sigma, \Phi)$. Finally, let $I = \{i \in \{1,\dots,n\} \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma\}$. We show that for all $i \in \{1,\dots,n\}$, Properties 1, 2, 3 and 6 of Definition 7 hold.

We first prove that for all term t such that $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(t)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P t$ implies $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$. Assume that P is minimal for $|P|$. We do a case analysis on $|P|$. If $|P| = 1$ then either $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$ or $t = \mathcal{E}_k\sigma$ for some $k \in \{1,\dots,n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(t)$. Hence, we deduce that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. Therefore, $\Phi \vdash t$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$.

Otherwise, $|P| > 1$. Let us assume that there exist $j \in \{1,\dots,n\}$ and $P' \in st(P)$ such that $P' = |\Phi| + j$. Since $|P| > 1$, we deduce that there exist $\mathsf{ir}, P'', P_1, \dots, P_m, \ell \in \{1,\dots,m\}$ such that $P'' = \mathsf{ir}(P_1,\dots,P_m) \in st(P)$ and $P_\ell = P'$. Let us denote t'' the term $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} t''$. By Lemma 19, we deduce that either $t'' \in st(\Phi) \cup st(\mathcal{E}_k\sigma)_{k=1}^n \cup st(t)$ or $t'' = \mathsf{g}(u)$ for some $\mathsf{g} \in \mathcal{F}_{key}$ and $u \in st_<(\Phi) \cup st_<(\mathcal{E}_k\sigma)_{k=1}^n \cup st_<(t)$. Since $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(t, \sigma, \Phi)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} \mathcal{E}_j\sigma$ and all $\mathcal{E}_1, \dots, \mathcal{E}_n$ are equal after variable renaming, we deduce that in both cases, ir cannot be a composition rule. Since ir is a decomposition rule, we in fact have $P'' = \mathsf{ir}(P', R)$ where ir the rule sign-decomp and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_R \mathsf{vk}(y_j\sigma)$. Moreover, we have $t'' = \langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x_j\sigma\rangle$. But it also implies that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_j\sigma$ meaning that $j \in I$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x_j\sigma\rangle$.

We have just shown that for all $j \in \{1,\dots,n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j and a term u such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} u$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{Q_j} u$. Therefore, by replacing all instances of $P|_{p'_j}$ in P by Q_j, we obtain that a proof P' such that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{P'} t$. This allows us to conclude.

Property 1: For all $i \in \{1,\dots,n\}$, for all $t \in \mathcal{T}(\mathcal{F}_{key}, \{y_i\sigma\}$, we have that $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(t)$. Hence we can apply the property we just proved which allows us to conclude.

Property 2: Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and $v \in st(\mathcal{E}_j) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\rangle$. By definition of $\mathcal{E}_{\mathsf{signcrypt}}$, u, v unifiable implies that there exists a position p of $\mathcal{E}_{\mathsf{signcrypt}}$ such that $u = \mathcal{E}_i|_p$ and $v = \mathcal{E}_j|_p$. Since $\mathcal{E}_i \sim \mathcal{E}_j$ then the result holds.

Property 3: We directly have that $\{\mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x\rangle, y), \mathsf{vk}(y)\} \vdash x$.

Property 6: Let $i \in \{1,\dots,n\}$. Let σ' some ground substitution such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$. Consider a proof P minimal for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P \mathcal{E}_i\sigma'$. If $|P| = 1$ then it implies that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}$ due to the fact that $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(\Phi)$. Therefore, there exists $k \in \{1,\dots,n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$. Since we already know that $\mathcal{E}_i \sim \mathcal{E}_k$ then the result holds.

Otherwise $|P| > 1$. In such a case $P = \mathsf{ir}(P_1,\dots,P_n)$. We do a case analysis on ir.

- Case ir is a decomposition rule: By Lemma 19, we deduce that $\mathcal{E}_i\sigma' \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n)$. But since $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(\Phi) \cup st(\sigma)$, then we deduce that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}^n$ which contradicts the minimality of $|P|$.

- Case ir is a composition rule: In such a case, we have $P = \mathsf{ir}(P_1, P_2)$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_1} \langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x_i\sigma' \rangle$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_2} z_i\sigma'$. Using the first property of the lemma, the result holds.

◀

B.5 MAC encapsulation

▶ **Lemma 24.** *Let* $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \in \mathsf{Tag}$. *Let* $\mathcal{E}_{\mathsf{mac}} = \langle x, \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x, y \rangle) \rangle$ *with* $\mathsf{t}_{\mathcal{E}_{\mathsf{mac}}} = x$ *and* $\mathsf{X}_{\mathcal{E}_{\mathsf{mac}}} = y$. *We have that* $(\mathcal{E}_{\mathsf{mac}}, \emptyset)$ *is a* $\{\mathsf{a}_{\mathcal{E}\mathsf{mac}}\}$*-tagged encapsulation and* $\mathcal{S} = \{(\mathcal{E}_{\mathsf{mac}}, \emptyset)\}$ *allows authentic channels.*

Proof. Let $(\mathcal{E}_1, \emptyset), \ldots, (\mathcal{E}_n, \emptyset) \in \mathcal{S}$ such that the variables of $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are disjoints. Since $\mathcal{S} = \{(\mathcal{E}_{\mathsf{signcrypt}}, \mathsf{vk}(y))\}$, we have that $\mathcal{E}_i \sim \mathcal{E}_j$ for all $i, j \in \{1, \ldots, n\}$. For all $i \in \{1, \ldots, n\}$, we will denote $\mathsf{t}_{\mathcal{E}_i} = x$ and $\mathsf{X}_{\mathcal{E}} = y_i$. Let σ be a ground substitution such that $dom(\sigma) \subseteq vars(\mathcal{E}_1, \ldots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(\sigma, \Phi)$. Finally, let $I = \{i \in \{1, \ldots, n\} \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma\}$. In fact we have $I = \{1, \ldots, n\}$. We show that for all $i \in \{1, \ldots, n\}$, Properties 1, 2, 3 and 6 of Definition 7 hold.

We first prove that for all term t such that $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(t)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P t$ implies $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$. Assume that P is minimal for $|P|$. We do a case analysis on $|P|$. If $|P| = 1$ then either $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$ or $t = \mathcal{E}_k\sigma$ for some $k \in \{1, \ldots, n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(t)$. Hence, we deduce that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. Therefore, $\Phi \vdash t$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$.

Otherwise, $|P| > 1$. Let us assume that there exist $j \in \{1, \ldots, n\}$ and $P' \in st(P)$ such that $P' = |\Phi| + j$. Since $|P| > 1$, we deduce that there exist ir, $P'', P_1, \ldots, P_m$, $\ell \in \{1, \ldots, m\}$ such that $P'' = \mathsf{ir}(P_1, \ldots, P_m) \in st(P)$ and $P_\ell = P'$. Let us denote t'' the term $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} t''$. By Lemma 19, we deduce that either $t'' \in st(\Phi) \cup st(\mathcal{E}_k\sigma)_{k=1}^n \cup st(t)$ or $t'' = \mathsf{g}(u)$ for some $\mathsf{g} \in \mathcal{F}_{key}$ and $u \in st_<(\Phi) \cup st_<(\mathcal{E}_k\sigma)_{k=1}^n \cup st_<(t)$. Since $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(t, \sigma, \Phi)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} \mathcal{E}_j\sigma$ and all $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are equal after variable renaming, we deduce that in both cases, ir cannot be a composition rule. Since ir is a decomposition rule, we in fact have $P'' = \mathsf{ir}(P')$ where ir is one of the decomposition of $\langle\ \rangle$, and so either $t'' = x_j\sigma$ or $t'' = \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x_j\sigma, y_j\sigma \rangle)$. If it is the latter then since $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(t)$, we deduce that $P \neq P''$ meaning that there exists $Q = \mathsf{ir}'(Q_1, \ldots, Q_\ell)$ and $\ell' \in \{1, \ldots, \ell\}$ such that $Q \in st(P)$ and $Q_{\ell'} = P''$. But there is no decomposition rule for h therefore ir′ is necessarily a composition rule.

By the Lemma 19, we can easily show that ir′ cannot be a composition rule for some $\mathsf{g} \notin \mathcal{F}_{key}$ since if would imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathcal{E}_r\sigma$ for some r which would contradict our hypothesis on the minimality of $|P|$. We also show that ir′ cannot be is a composition rule for some $\mathsf{g} \in \mathcal{F}_{key}$. In such a case, it would imply that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_Q \mathsf{g}(t'')$. But since $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \in st(t'')$, then $Q \neq P$ and so there must be another inference rule ir′′ applied on Q in P. Once again, by Lemma 19, ir′′ cannot be a composition rule for any function symbol since it would imply that $\mathsf{g}(t'') \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n) \cup st(t)$ but $\mathcal{E}_{\mathsf{mac}}$ does not contain function symbol from $\mathcal{F}_{key}$ and $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(t, \sigma, \Phi)$. Moreover, ir′′ cannot be a decomposition rule either since the only rule involving a function symbol $\mathsf{g} \in \mathcal{F}_{key}$ as argument is the signature decomposition which would imply that there exists a term v and a proof $R \in st(P)$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_R \mathsf{sign}(v, t'')$. Once again, this is prevented by Lemma 19. Therefore, we can conclude that ir′ cannot be a composition rule for some $\mathsf{g} \in \mathcal{F}_{key}$.

We just have proven that if $t'' = \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x_j\sigma, y_j\sigma \rangle)$ then ir′ cannot be a composition nor a decomposition rule which is a contradiction. Hence $t'' = x_j\sigma$. Therefore, we have just shown that for all $j \in \{1, \ldots, n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j and a proof Q_j such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} x_j\sigma$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{Q_j} x_\sigma$. Therefore, by replacing all instances of $P|_{p'_j}$ in P by Q_j, we obtain that a proof P' such that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{P'} t$. This allows us to conclude.

Property 1: For all $i \in \{1,\dots,n\}$, for all $t \in \mathcal{T}(\mathcal{F}_{key}, \{y_i\sigma\}$, we have that $\mathsf{a}_{\mathcal{E}\mathsf{sign}} \notin st(t)$. Hence we can apply the property we just proved which allows us to conclude.

Property 2: Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and $v \in st(\mathcal{E}_j) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\rangle$. By definition of $\mathcal{E}_{\mathsf{signcrypt}}$, u, v unifiable implies that there exists a position p of $\mathcal{E}_{\mathsf{signcrypt}}$ such that $u = \mathcal{E}_i|_p$ and $v = \mathcal{E}_j|_p$. Since $\mathcal{E}_i \sim \mathcal{E}_j$ then the result holds.

Property 3: We directly have that $\{\langle x, \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x, y\rangle)\rangle\} \vdash x$.

Property 6: Let $i \in \{1,\dots,n\}$. Let σ' some ground substitution such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$. Consider a proof P minimal for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P \mathcal{E}_i\sigma'$. If $|P| = 1$ then it implies that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}$ due to the fact that $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(\Phi)$. Therefore, there exists $k \in \{1,\dots,n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$. Since we already know that $\mathcal{E}_i \sim \mathcal{E}_k$ then the result holds.

Otherwise $|P| > 1$. In such a case $P = \mathsf{ir}(P_1,\dots,P_n)$. We do a case analysis on ir.

- Case ir is a decomposition rule: By Lemma 19, we deduce that $\mathcal{E}_i\sigma' \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n)$. But since $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(\Phi) \cup st(\sigma)$, then we deduce that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}^n$ which contradicts the minimality of $|P|$.
- Case ir is a composition rule: In such a case, we have $P = \mathsf{ir}(P_1, P_2)$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_1} x_i\sigma'$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P_2} \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x_i\sigma', y_i\sigma'\rangle)$. Let us focus on P_2. Since $\mathsf{a}_{\mathcal{E}\mathsf{mac}} \notin st(\Phi, \sigma)$, we have that P_2 starts by either a decomposition rule or a composition rule. If it is the latter then we have that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash y\sigma'$ and so the result would hold with the first property of the lemma. If it is the former, then by Lemma 19, we would have that $\mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x_i\sigma', y_i\sigma'\rangle) \in st(\{\mathcal{E}_k\sigma\}_{k=1}^)$. It would imply that there exists $k \in \{1,\dots,n\}$ such that $x_k\sigma = x_i\sigma'$ and $y_k\sigma = y_i\sigma'$. Hence with the first property of the lemma, the result holds.

◀

B.6 Aenc encapsulation

▶ **Lemma 25.** *Let* $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \in \mathsf{Tag}$. *Let* $\mathcal{E}_{\mathsf{TLS}} = \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{aenc}}, x\rangle, \mathsf{pk}(y))$, $\mathsf{t}_{\mathcal{E}_{\mathsf{aenc}}} = x$ *and* $\mathsf{X}_{\mathcal{E}_{\mathsf{aenc}}} = y$. *We have that* $(\mathcal{E}_{\mathsf{aenc}}, \mathsf{pk}(y))$ *is a* $\{\mathsf{a}_{\mathcal{E}\mathsf{aenc}}\}$*-tagged encapsulation and* $\mathcal{S} = \{(\mathcal{E}_{\mathsf{TLS}}, \mathsf{pk}(y))\}$ *allows confidential channels.*

Proof. Let $(\mathcal{E}_1, \emptyset), \dots, (\mathcal{E}_n, \emptyset) \in \mathcal{S}$ such that the variables of $\mathcal{E}_1, \dots, \mathcal{E}_n$ are disjoints. Since $\mathcal{S} = \{(\mathcal{E}_{\mathsf{TLS}}, \emptyset)\}$, we have that $\mathcal{E}_i \sim \mathcal{E}_j$ for all $i, j \in \{1,\dots,n\}$. For all $i \in \{1,\dots,n\}$, we will denote $\mathsf{t}_{\mathcal{E}_i} = x_i$ and $\mathsf{X}_{\mathcal{E}_i} = y_i$. Let σ be a ground substitution such that $dom(\sigma) \subseteq vars(\mathcal{E}_1, \dots, \mathcal{E}_n)$ and let Φ be a ground frame such that $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(\sigma, \Phi)$. Finally, let $I = \{i \in \{1,\dots,n\} \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma\}$. We show that for all $i \in \{1,\dots,n\}$, Properties 1, 2, 4 and 5 of Definition 7 hold.

Property 1: Let $i \in \{1,\dots,n\}$. Let $t \in \mathcal{T}(\mathcal{F}_{key}, \{y_i\sigma\})$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P t$. Assume that P is minimal for $|P|$. We do a case analysis on $|P|$. If $|P| = 1$ then either $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$ or $t = \mathcal{E}_k\sigma$ for some $k \in \{1,\dots,n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{TLS}} \notin st(t)$. Hence, we deduce that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $t \in \Phi$. Therefore, $\Phi \vdash t$ and so $\Phi \cdot [x_k\sigma]_{k\in I} \vdash t$.

Otherwise, $|P| > 1$. Let us assume that there exists $j \in \{1,\dots,n\}$ and $P' \in st(P)$ such that $P' = |\Phi| + j$. Since $|P| > 1$, we deduce that there exists $\mathsf{ir}, P'', P_1, \dots, P_m, \ell \in \{1,\dots,m\}$ such that $P'' = \mathsf{ir}(P_1,\dots,P_m) \in st(P)$ and $P_\ell = P'$. Let us denote t'' the term $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} t''$. By Lemma 19, we deduce that either $t'' \in st(\Phi) \cup st(\mathcal{E}_k\sigma)_{k=1}^n \cup st(t)$ or $t'' = \mathsf{g}(u)$ for some $\mathsf{g} \in \mathcal{F}_{key}$ and $u \in st_<(\Phi) \cup st_<(\mathcal{E}_k\sigma)_{k=1}^n \cup st_<(t)$. Since $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(t, \sigma, \Phi)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P'} \mathcal{E}_j\sigma$ and all $\mathcal{E}_1, \dots, \mathcal{E}_n$ are equal after variable renaming, we deduce that in both cases, ir cannot be a composition rule. Therefore ir is the decomposition rule of aenc and we have $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} \langle \mathsf{a}_{\mathcal{E}\mathsf{aenc}}, x_j\sigma\rangle$. Thus $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P''} \langle x_j\sigma$ and so $j \in I$. Hence, $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x_j\sigma\rangle$.

We have just shown that for all $j \in \{1,\dots,n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j and a term u such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} u$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{Q_j} u$. Therefore, by replacing all instances of $P|_{p'_j}$ in P by Q_j, we obtain that a proof P' such that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash_{P'} t$. This allows us to conclude.

Property 2: Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and $v \in st(\mathcal{E}_j) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\rangle$. By definition of $\mathcal{E}_{\mathsf{aenc}}$, u, v unifiable implies that there exists a position p of $\mathcal{E}_{\mathsf{TLS}}$ such that $u = \mathcal{E}_i|_p$ and $v = \mathcal{E}_j|_p$. Since $\mathcal{E}_i \sim \mathcal{E}_j$ then the result holds.

Property 4: Let $i \in \{1,\dots,n\}$. Consider a minimal proof P for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P x_i\sigma$. We do a case analysis on $|P|$. If $|P| = 1$ then either $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$ or $x_i\sigma = \mathcal{E}_k\sigma$ for some $k \in \{1,\dots,n\}$. But $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(x_i\sigma)$. Hence, we deduce that $x_i\sigma \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ or $x_i\sigma \in \Phi$. Therefore, $\Phi \vdash x_i\sigma$ and so $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_i\sigma$.

Otherwise, $|P| > 1$. Following exactly the proof of Property 1 (replacing t by $x_i\sigma$), we deduce that for all $j \in \{1,\dots,n\}$, for all position p_j of P, if $P|_{p_j} = |\Phi| + j$ then there exists a prefix p'_j of p_j, a proof Q_j such that $P|_{p'_j} = \mathsf{ir}_1(|\Phi| + j, Q_j)$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{P|_{p'_j}} \langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x_j\sigma\rangle$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_{Q_j} y_j\sigma$ where ir_1 is the decomposition rule of aenc. Let us look at the proof Q_j. Since $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(y_j\sigma)$, we can deduce by minimality of $|P|$ that $|\Phi| + j \notin Q_j$ (otherwise, using the same reasoning, it would imply that there exists a proof $Q'_j \in st_<(Q_j)$ deducing $y_i\sigma$). Thus, $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash_{Q_j} y_j\sigma$. Let $I' = \{i \in \{1,\dots,n\} - j \mid \Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j} \vdash x_i\sigma\}$. Note that $I' \subseteq I - j$. By applying Property 1 on $y_j\sigma$ with $[\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}-j}$ and I', we deduce that $\Phi \cdot [x_k\sigma]_{k\in I'} \vdash y_j\sigma$.

Therefore, we have proven that if $|\Phi| + i \in st(P)$ then $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash y_i\sigma$. Otherwise, if for all $j \in \{1,\dots,n\}$, for all position p_j of P, $P|_{p_j} = |\Phi| + j$ implies that $i \neq j$ then we also have proven that $\Phi \cdot [x_k\sigma]_{k\in I-i} \vdash x_j\sigma$ using the same replacement of proofs as in the proof of Property 1. Hence, the result holds.

Property 5: Let $i \in \{1,\dots,n\}$. Let σ' be some ground substitution such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_i\sigma'$ and $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(\sigma')$. We focus first on the left implication of the equivalence. If $\Phi \cdot [x_k\sigma]_{k\in I} \vdash x_i\sigma'$ and $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \mathsf{pk}(y_i)\sigma'$ then we directly have that $\Phi \cdot [x_k\sigma]_{k\in I} \vdash \mathcal{E}_i\sigma'$. But since for all $k \in I$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}} \vdash x_k\sigma$, we deduce that $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}} \vdash \mathcal{E}_i\sigma'$. Otherwise, there exists $j \in \{1,\dots,n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_j\sigma$ and so we directly have that $\Phi \cdot [\mathcal{E}_k\sigma]_{k\in\{1,\dots,n\}} \vdash \mathcal{E}_i\sigma'$.

Let us now focus on the right implication of the equivalence. Consider a proof P minimal for $|P|$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash_P \mathcal{E}_i\sigma'$. If $|P| = 1$ then it implies that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}$ due to the fact that $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(\Phi)$. Therefore, there exists $k \in \{1,\dots,n\}$ such that $\mathcal{E}_i\sigma' = \mathcal{E}_k\sigma$. Since we already know that $\mathcal{E}_i \sim \mathcal{E}_k$ then the result holds.

Otherwise $|P| > 1$. In such a case $P = \mathsf{ir}(P_1,\dots,P_n)$. We do a case analysis on ir.

- Case ir is a decomposition rule: by Lemma 19, we deduce that $\mathcal{E}_i\sigma' \in st(\Phi) \cup st([\mathcal{E}_k\sigma]_{k=1}^n)$. But since $\mathsf{a}_{\mathcal{E}\mathsf{aenc}} \notin st(\Phi) \cup st(\sigma)$, then we deduce that $\mathcal{E}_i\sigma' \in [\mathcal{E}_k\sigma]_{k=1}^n$ which contradicts the minimality of $|P|$.
- Case ir is a composition rule: Then we directly have that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash x_i\sigma'$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{pk}(y_i\sigma')$. Once again by following the same proof as in Property 1 (replacing t by $x_i\sigma'$), we deduce that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash x_i\sigma'$ and $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash \mathsf{pk}(y_i\sigma')$ and so the result holds.

◀

B.7 Proof of Theorem 8

▶ **Lemma 26.** *Let $\mathcal{S}_e$ be a set of* Tag*-encapsulations allowing authentic, confidential and secure channels. Let Φ be a ground frame and σ be a ground substitution such that* $\mathsf{Tag} \cap st(\sigma, \Phi) = \emptyset$*. Let $(\mathcal{E}_1, \mathsf{F}_1), \dots, (\mathcal{E}_n, \mathsf{F}_n) \in \mathcal{S}_e$. Assume that the variables in $\mathcal{E}_1, \dots, \mathcal{E}_n$ are disjoint. Let I be the set of*

$i \in \{1,\dots,n\}$ *such that* $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. *For all terms* t, *if* $\mathsf{Tag} \cap st(t) = \emptyset$ *and* $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash t$ *then* $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash t$.

Proof. Consider $(\mathcal{E}_{n+1}, \mathsf{F}_{n+1}) \in \mathcal{S}_e$ such that the variables of $\mathcal{E}_{n+1}$ are disjoint from $\mathcal{E}_1,\dots,\mathcal{E}_n$. Take σ' the ground substitution such that $\mathsf{t}_{\mathcal{E}_{n+1}}\sigma' = a \in \mathcal{N}_D$ and for all $x \in \mathsf{X}_{\mathcal{E}_{n+1}}$, $x\sigma' = t$. Since $\mathsf{Tag} \cap st(t) = \emptyset$, we deduce that $\mathsf{Tag} \cap st(\sigma\sigma') = \emptyset$. Moreover, we have $t \in \mathcal{T}(\mathcal{F}_{key}, \mathsf{X}_{\mathcal{E}_{n+1}}\sigma\sigma')$.

We also that that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash t$ implies that $\Phi \cdot [\mathcal{E}_k\sigma\sigma']_{k=1}^n \vdash t$ which implies $\Phi \cdot [\mathcal{E}_k\sigma\sigma']_{k=1}^{n+1} \vdash t$. On the other hand, since $a \in \mathcal{N}_D$ and for all $x \in \mathsf{X}_{\mathcal{E}_{n+1}}$, $x\sigma' = t$ with $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash t$, we deduce that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathcal{E}_{n+1}\sigma'$. Hence for all $i \in \{1,\dots,n\}$, if $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ then $\Phi \cdot [\mathcal{E}_k\sigma\sigma']_{k=1}^{n+1} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$.

Thus by applying Property 1 of Definition 7, we deduce that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma\sigma']_{k\in I} \vdash t$ and so $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash t$. ◂

▸ **Lemma 27.** *Let* $\mathcal{S}_e$ *be a set of* tag_A*-encapsulations allowing authentic, confidential and secure channels. Let* $\mathcal{S}'_e$ *be a set of* tag_B*-encapsulations allowing authentic, confidential and secure channels. If* $\mathsf{tag}_A \cap \mathsf{tag}_B = \emptyset$ *then* $\mathcal{S}_e \cup \mathcal{S}'_e$ *is a set of* $\mathsf{tag}_A \cup \mathsf{tag}_B$*-encapsulations allowing authentic, confidential and secure channels.*

Proof. Let $(\mathcal{E}_1, \mathsf{F}_1),\dots,(\mathcal{E}_n, \mathsf{F}_n) \in \mathcal{S}_e \cup \mathcal{S}'_e$. Assume that the variables in $\mathcal{E}_1,\dots,\mathcal{E}_n$ are disjoint. Let σ be a ground substitution such that $dom(\sigma) = vars(\mathcal{E}_1,\dots,\mathcal{E}_n)$ and let Φ be a ground frame such that $(\mathsf{tag}_A \cup \mathsf{tag}_B) \cap st(\sigma,\Phi) = \emptyset$. Let I be the set of $i \in \{1,\dots,n\}$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. Let us denote by $A = \{i \in \{1,\dots,n\} \mid (\mathcal{E}_i, \mathsf{F}_i) \in \mathcal{S}_e\}$ and $B = \{i \in \{1,\dots,n\} \mid (\mathcal{E}_i, \mathsf{F}_i) \in \mathcal{S}'_e\}$. Moreover, let us denote by $I_A = I \cap A$ and $I_B = I \cap B$. We first start proving the following property:

Property 0: For all term t, if $(\mathsf{tag}_A \cup \mathsf{tag}_B) \cap st(t) = \emptyset$ and $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash t$ then $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash t$.

Assume w.l.o.g. that $i \in A$. Let us denote $\Phi' = \Phi \cdot [\mathcal{E}_k\sigma]_{k\in B}$. We have $\Phi' \cdot [\mathcal{E}_k\sigma]_{k\in A} \vdash t$. But $(\mathsf{tag}_A \cup \mathsf{tag}_B) \cap st(\sigma,\Phi) = \emptyset$ and so $\mathsf{tag}_A \cap st(\sigma,\Phi) = \emptyset$. Moreover, I_A is the set of $i \in A$ such that $\Phi' \cdot [\mathcal{E}_k\sigma]_{k\in A} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. Since $\mathcal{S}_e$ be a set of tag_A-encapsulations allowing authentic, confidential and secure channels, we deduce by Lemma 26 that $\Phi' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A} \vdash t$.

If now we denote $\Phi'' = \Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A}$, we obtain that $\Phi'' \cdot [\mathcal{E}_k\sigma]_{k\in B} \vdash t$. Consider the set I'_B of $i \in B$ such that $\Phi'' \cdot [\mathcal{E}_k\sigma]_{k\in B} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. We show that $I'_B = I_B$. If $i \in I_B$ then we know that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. By applying onc again Lemma 26 on Φ', A and I_A, we deduce that $\Phi' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ and so $\Phi'' \cdot [\mathcal{E}_k\sigma]_{k\in B} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ meaning that $i \in I'_B$. If $i \in I'_B$, we know that $\Phi'' \cdot [\mathcal{E}_k\sigma]_{k\in B} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ and so $\Phi' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. But for all $j \in I_A$, $\Phi' \cdot [\mathcal{E}_k\sigma]_{k\in A} \vdash \mathsf{t}_{\mathcal{E}_j}\sigma$. Hence we deduce that $\Phi' \cdot [\mathcal{E}_k\sigma]_{k\in A} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ and so $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. This allows us to conclude that $I_B = I'_B$. Thus, we can apply Lemma 26 on Φ'', I_B and t which allows us to deduce that $\Phi'' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_B} \vdash t$ and so we conclude that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I} \vdash t$.

Property 1: Direct application of Property 0.

Property 2: Let $i, i' \in \{1,\dots,n\}$. Let $u \in st(\mathcal{E}_i) \setminus \mathcal{X}$ and let $v \in st(\mathcal{E}_{i'}) \setminus \mathcal{X}$ such that u and v are unifiable and $\mathsf{root}(u) \neq \langle\,\rangle$. Thus $\mathsf{tag}_A \cap \mathsf{tag}_B = \emptyset$, we deduce that either $i, i' \in A$ or $i, i' \in B$. In such a case the result directly holds by applying Property 2 of Definition 7 on either A or B.

Property 3: Direct from Definition 7.

Property 4: Let $i \in \{1,\dots,n\}$ such that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. Assume w.l.o.g. that $i \in A$. Let us denote $\Phi' = \Phi \cdot [\mathcal{E}_k\sigma]_{k\in B}$. Thus by applying Property 4 of Definition 7 on Φ', σ, I_A, we deduce that $\Phi' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A - i} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$ or there exists $x \in \mathsf{X}_{\mathcal{E}_i}$ such that $\Phi' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A - i} \vdash x\sigma$.

Let us $\Phi'' = \Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A - i}$. Consider I'_B the set of $j \in B$ such that $\Phi'' \cdot [\mathcal{E}_k\sigma]_{k\in B} \vdash \mathsf{t}_{\mathcal{E}_j}\sigma$. We know that for all $k \in I_A - i$, $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_k}\sigma$. Therefore, we deduce that $\Phi \cdot [\mathcal{E}_k\sigma]_{k=1}^n \vdash \mathsf{t}_{\mathcal{E}_j}\sigma$ and so $I'_B \subseteq I_B$. Hence by applying Lemma 26 on Φ'', I'_B and $x\sigma$ or $\mathsf{t}_{\mathcal{E}_i}\sigma$, we deduce that $\Phi'' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I'_B} \vdash x\sigma$ or $\Phi'' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I'_B} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. But considering that $I'_B \subseteq I_B$, we deduce that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I-i} \vdash x\sigma$ or $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I-i} \vdash \mathsf{t}_{\mathcal{E}_i}\sigma$. Hence the result holds.

Property 5 and 6: Similar proof as Property 4, that is we assume w.l.o.g. that $i \in A$, we apply Property 5 (resp. 6) on the frame $\Phi' = \Phi \cdot [\mathcal{E}_k\sigma]_{k\in B}$ and I_A, and when we are in the case of $\Phi' \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A}$ deduces a term u, we use Lemma 26 on $\Phi'' = \Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I_A}$, I_B and u to obtain that $\Phi \cdot [\mathsf{t}_{\mathcal{E}_k}\sigma]_{k\in I}$ deduce u. ◂

▸ **Theorem 8.** *The following encapsulations are:*

authentic: $\mathcal{E}_{\mathsf{sign}} = \mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}\mathsf{sign}}, x\rangle, x_1)$ *and* $\mathcal{E}_{\mathsf{mac}} = \langle x, \mathsf{h}(\langle \mathsf{a}_{\mathcal{E}\mathsf{mac}}, x, x_1\rangle)\rangle$*;*
confidential: $\mathcal{E}_{\mathsf{aenc}} = \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{aenc}}, x\rangle, \mathsf{pk}(x_1))$*;*
secure: $\mathcal{E}_{\mathsf{TLS}} = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, x\rangle, x_1)$, $\mathcal{E}_{\mathsf{BAC}} = \langle t, \mathsf{mac}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, t\rangle, x_2)\rangle$ *with* $t = \mathsf{senc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, x\rangle, x_1)$, *and* $\mathcal{E}_{\mathsf{signcrypt}} = \mathsf{sign}(\langle \mathsf{a}_{\mathcal{E}\mathsf{signcrypt}}, \mathsf{aenc}(\langle \mathsf{a}_{\mathcal{E}\mathsf{signcrypt}}, x\rangle, \mathsf{pk}(x_1))\rangle, x_2)$.

where $\mathsf{a}_{\mathcal{E}\mathsf{sign}}, \mathsf{a}_{\mathcal{E}\mathsf{mac}}, \mathsf{a}_{\mathcal{E}\mathsf{aenc}}, \mathsf{a}_{\mathcal{E}\mathsf{TLS}}, \mathsf{a}_{\mathcal{E}\mathsf{BAC}}, \mathsf{a}_{\mathcal{E}\mathsf{signcrypt}}$ *are constants.*

Moreover, the set $\{(\mathcal{E}_{\mathsf{sign}}, \{\mathsf{vk}(x_1)\}), (\mathcal{E}_{\mathsf{mac}}, \emptyset), (\mathcal{E}_{\mathsf{aenc}}, \{\mathsf{pk}(x_1)\}), (\mathcal{E}_{\mathsf{TLS}}, \emptyset), (\mathcal{E}_{\mathsf{BAC}}, \emptyset), (\mathcal{E}_{\mathsf{signcrypt}}, \emptyset)\}$ *allowsfor authentic, confidential and secure channels.*

Proof. Lemmas 20, 21, 22, 23, 25 and 24 give us that the encapsulations individually allows secure, confidential, authentic channels. Thus the proof is concluded by successive applications of Lemma 27 since all the encapsulations are tagged differently. ◂

C Proofs of Theorem 17

C.1 Properties on the composed frame

We say that a term t is a tag_A-term if $t = \mathsf{f}(\langle \mathsf{a}, t_1\rangle, t_2, \ldots, t_n)$ where $\mathsf{a} \in \mathsf{tag}_A$ for some $t_1, \ldots, t_n$.

▸ **Definition 28.** Let $\mathcal{S}$ be a set of tag_A-tagged encapsulations. Let $\Phi = [u_1; \ldots; u_n]$ be a frame. Let $I \subseteq \{1, \ldots, n\}$. We say that Φ *is an executed frame for* $\mathcal{S}$ *and* I if:

- for all $i \in I$, $u_i = \mathcal{E}_i\Sigma_i$ for some ground substitutions Σ_i and some encapsulation $(\mathcal{E}_i, \mathsf{F}_i) \in \mathcal{S}$; and
- for all $i \in I$ (resp $i \notin I$), for all $t \in vars(\mathcal{E}_i)\Sigma_i$ (resp. $t \in \{u_i\}$), for all positions p of t, if $t|_p$ is a tag_A-term then:
  - either $p = p' \cdot a \cdot p''$ for some position p', p'' and there exists $j \in I$ such that $j < i$, $t|_{p'\cdot a}, t|_p \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$ and $[u_1; \ldots; u_{i-1}] \vdash t|_{p'\cdot a}$;
  - or $[u_1; \ldots; u_{i-1}] \vdash t|_p$.

▸ **Corollary 29.** *Let* $\mathcal{S}$ *be a set of* tag_A*-tagged encapsulations. Let* $\Phi = [u_1; \ldots; u_n]$ *be an executed frame for* $\mathcal{S}$ *and some set* I. *For all* $k \in \{1, \ldots, n\}$, $[u_1; \ldots; u_k]$ *is an executed frame for* $\mathcal{S}$ *and* $I \setminus \{k+1; \ldots; n\}$.

In the rest of the section, if $\Phi = [u_1; \ldots; u_n]$ is an executed frame for $\mathcal{S}$ and I then for all $i \in I$, we will always denote by $\mathcal{E}_i\Sigma_i$ the term u_n as described in the above definition.

▸ **Lemma 30.** *Let* $\mathcal{S}$ *be a set* tag_A*-tagged encapsulations. Let* Φ *be a frame and* $I \subseteq \{1, \ldots, |\Phi|\}$. *Assume that* Φ *is an executed frame for* $\mathcal{S}$ *and* I. *We have that for all* $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$, *if* $\Phi \vdash t$ *then for all positions* p *of* t, *if* $t|_p$ *is a* tag_A*-term then:*

- *either* $p = p' \cdot a \cdot p''$ *for some position* p', p'' *and there exists* $j \in I$ *such that* $t|_{p'\cdot a}, t|_p \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$ *and* $\Phi \vdash t|_{p'\cdot a}$*;*
- *or* $\Phi \vdash t|_p$.

Proof. Let us denote by P the minimal proof such that $\Phi \vdash_P t$. Let us denote $\Phi = [u_1; \ldots; u_n]$. We prove this result by induction $|P|$.

Base case $|P| = 1$*:* In such a case, either $t \in \mathcal{N}_D$ or there exists $i \notin I$ such that $t = u_i$ or there exists $i \in I$ such that $t = \mathcal{E}_i\Sigma_i$. However, In the first case, the result trivially holds.

In the second case, by Definition 28, we know that for all positions p of t, if $t|_p$ is a tag_A-term then:

- either $p = p' \cdot a \cdot p''$ for some position p', p'' and there exists $j \in I$ such that $j < i$, $t|_{p'\cdot a}, t|_p \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$ and $[u_1; \ldots; u_{i-1}] \vdash t|_{p'\cdot a}$ which implies that $\Phi \vdash t|_{p'\cdot a}$
- or $[u_1; \ldots; u_{i-1}] \vdash t|_p$ which implies that $\Phi \vdash t|_p$.

Therefore the result holds.

In the third case, for all positions p of $\mathcal{E}_i\Sigma_i$, we distinguish whether $t|_p \in st(\mathcal{E}_i\Sigma_i) \setminus st(\Sigma_i)$ or not. In the latter, it implies that $t|_p \in st(\Sigma_i)$ and so there exists $t' \in vars(\mathcal{E}_i)\Sigma_i$ and a position p' such that $t'|_{p'} = t|_p$ and p' is a suffix or p. Therefore, by Definition 28 (instantiating t and p of the definition by t' and p' respectively), we obtain that if $t'|_{p'}$ is a tag_A-term then:

- either $p' = p'' \cdot a \cdot p'''$ for some position p'', p''' and there exists $j \in I$ such that $j < i$, $t'|_{p''\cdot a}, t'|_{p'} \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$ and $[u_1; \ldots; u_{i-1}] \vdash t|_{p'\cdot a}$. Since p' is a suffix of p then $p = q \cdot p'$ for some q. And so we obtain that $p = (q \cdot p'') \cdot a \cdot p'''$, $t|_{(q\cdot p'')\cdot a}, t|_p \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$ and $\Phi \vdash t|_p$. Hence the result holds.
- or $[u_1; \ldots; u_{i-1}] \vdash t|_p$ which implies that $\Phi \vdash t|_p$.

In the former case, that is $t|_p \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$, the result directly holds since $t = \mathcal{E}_i\Sigma_i$ and $\Phi \vdash t$.

Inductive step $|P| > 1$ *and the last rule of* P *is a composition:* In such a case, $t = \mathsf{f}(t_1, \ldots, t_m)$ and for all $i \in \{1, \ldots, m\}$, $\Phi \vdash t_i$. Therefore, we can apply our inductive hypothesis on all $t_1, \ldots, t_n$ which allows us to conclude for all position p of t different from ε. However, in the case where $p = \varepsilon$, we know by hypothesis that $\Phi \vdash t$ and so the result trivially holds.

Inductive step $|P| > 1$ *and the last rule of* P *is a decomposition:* Since P is minimal, we know that there exists $i \in \{1, \ldots, n\}$ such that $t \in st(u_i)$. Thus, we can apply the same reasoning as in the base case $|P| = 1$. This allows us to conclude. ◂

▸ **Definition 31.** Let $\mathcal{S}$ be a set tag_A-tagged encapsulations. Let Φ be a frame and $I \subseteq \{1, \ldots, |\Phi|\}$. Assume that Φ is an executed frame for $\mathcal{S}$ and I. Let σ be a substitution. We say that σ *is an executed substitution for* Φ if for all $t \in img(\sigma)$, for all positions p of t, if $t|_p$ is a tag_A-term then:

- either $p = p' \cdot a \cdot p''$ for some position p', p'' and there exists $j \in I$ such that $t|_{p'\cdot a}, t|_p \in st(\mathcal{E}_j\Sigma_j) \setminus st(\Sigma_j)$ and $\Phi \vdash t|_{p'\cdot a}$;
- or $\Phi \vdash t|_p$.

C.2 Transformation on composition frame and encapsulations

▸ **Definition 32.** Let δ be a mapping from terms to nonces. We define the application of δ on a term u, denoted $\mathsf{Ap}_\delta(u)$, as follows:

- if $u \in dom(\delta)$ then $\mathsf{Ap}_\delta(u) = u\delta$;
- else if $u \in \mathcal{N} \cup \mathcal{X}$ then $\mathsf{Ap}_\delta(u) = u$;
- else $u = \mathsf{f}(u_1, \ldots, u_n)$ and $\mathsf{Ap}_\delta(u) = \mathsf{f}(\mathsf{Ap}_\delta(u_1), \ldots, \mathsf{Ap}_\delta(u_n))$ for some $\mathsf{f}, u_1, \ldots, u_n$.

▸ **Definition 33.** We say that δ is a tag_A*-mapping of a frame* Φ when $names(\Phi) \cap img(\delta) = \emptyset$, $img(\delta) \in \mathcal{N}_D$ and $dom(\delta) \supseteq \{t \in st(\Phi) \mid t \text{ is a } \mathsf{tag}_A\text{-term}\}$.

▶ **Lemma 34.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations allowing authentic, confidential and secure channels. Let $(\mathcal{E}, \ell, S) \in \mathcal{S}$. For all substitution Σ, for all tag_A-mapping δ of $[\mathcal{E}\Sigma]$, for all position p of $\mathcal{E}$, there exists a context $C[\_]$ built on $\{\langle\,\rangle\} \cup \mathcal{F}_{cst}$ (possibly just a hole) such that*

- $\mathcal{E}\Sigma|_p = C[u_1, \ldots, u_n]$;
- *for all $i \in \{1, \ldots, n\}$, u_i is either a tag_A-term of $dom(\delta)$ or $u_i \in vars(\mathcal{E})\Sigma$ or a term of the form $\mathsf{f}(v)$ for some $\mathsf{f} \in \mathcal{F}_{key}$ and $v \in \mathsf{X}_{\mathcal{E}}\Sigma \cup \mathcal{F}_{cst}$.*
- $\mathsf{Ap}_\delta(\mathcal{E}\Sigma|_p) = C[\mathsf{Ap}_\delta(u_1), \ldots, \mathsf{Ap}_\delta(u_n)]$;
- $\mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p = C[v_1, \ldots, v_n]$;
- *for all $i \in \{1, \ldots, \ell\}$, u_i is (resp. not) a tag_A-term implies v_i is a tag_A-term (resp. $v_i = \mathsf{Ap}_\delta(u_i)$).*

Proof. By Definition 5, we know that $\mathcal{E}$ is a fully tag_A-term of $\mathcal{T}(\mathcal{F}, \{x, x_1, \ldots, x_n\})$ such that for all $t \in st(\mathcal{E})$,

- if $\mathsf{root}(t) = \mathsf{f} \in \mathcal{F}_{key}$ then $t = \mathsf{f}(y)$ with $y \in \{x_1, \ldots, x_n\} \cup \mathcal{F}_{cst}$
- if $t = \mathsf{f}(t', t_1, \ldots, t_n)$ and there exists an inference rule $\mathsf{ir}(\mathsf{f}(y, u_1, \ldots, u_n), v_1, \ldots, v_m) \to y$ then for all $j \in \{1, \ldots, m\}$, for all $i \in \{1, \ldots, n\}$, $v_j = \mathsf{g}(u_i)$ implies that $t_i \in \{x, x_1, \ldots, x_\ell\}$.

Let $t, s_1, \ldots, s_\ell$ be some terms. We prove the different properties by induction on $H - |p|$ where H is the maximal size of all positions in $\mathcal{E}$.

Base case $|p| > H$: Such a case is impossible since H is the maximal size of all positions in $\mathcal{E}$.

Inductive case $|p| \leq H$: By Definition of a fully tag_A-term, we know that either $\mathsf{root}(\mathcal{E}|_p) \in \mathcal{F}_{cst} \cup \{x, x_1, \ldots, x_n, \langle\,\rangle\}$ or $\mathcal{E}|_p$ is a tag_A-term. We do a case analysis. If $\mathsf{root}(\mathcal{E}|_p) \in \mathcal{F}_{cst}$ then the result trivially holds with $C = \mathcal{E}$. If $\mathsf{root}(\mathcal{E}|_p) \in \{x, x_1, \ldots, x_n\}$ then the result trivially holds with $C = \_$. If $\mathsf{root}(\mathcal{E}|_p) = \langle\,\rangle$ then $\mathcal{E}|_p = \langle \mathcal{E}|_{p\cdot 1}, \mathcal{E}|_{p\cdot 2}\rangle$. It implies that $\mathsf{Ap}_\delta(\mathcal{E}|_p\Sigma) = \langle \mathsf{Ap}_\delta(\mathcal{E}|_{p\cdot 1}\Sigma), \mathsf{Ap}_\delta(\mathcal{E}|_{p\cdot 2}\Sigma)\rangle$ and that $\mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p = \langle M_1, M_2\rangle$ with $M_1 = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_{p\cdot 1}$ and $M_2 = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_{p\cdot 2}$. Therefore, we can apply our inductive hypothesis on $p \cdot 1$ and $p \cdot 2$ which show the existence of a context C_1 and C_2 satisfying their respective properties. We conclude with $C = \langle C_1, C_2\rangle$. Lastly, if $\mathcal{E}|_p$ is a tag_A-term, then $\mathcal{E}|_p = \mathsf{f}(\langle \mathsf{a}, \mathcal{E}|_{p\cdot 1\cdot 2}\rangle, \mathcal{E}|_{p\cdot 2}, \ldots, \mathcal{E}|_{p\cdot m})$ for some $\mathsf{a} \in \mathsf{tag}_A$ and some integer m. Therefore, $\mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p$ is also a tag_A-term. Hence the result holds with $C = \_$. ◀

▶ **Lemma 35.** *Let $(\mathcal{E}, \mathsf{F})$ be a tag_A-tagged encapsulation. Let Σ be a ground substitution. Let δ be a tag_A-mapping of $[\mathcal{E}\Sigma]$. For all position p of $\mathcal{E}$, if there exists a term t such that $names(t) \cap img(\delta) = \emptyset$ and $\mathsf{Ap}_\delta(t) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p$ then $\mathcal{E}|_p$ does not contain tag_A-tagged term and $t = \mathcal{E}\Sigma|_p$.*

Proof. We prove the result by a downward induction on $|p|$:

Base case $\mathcal{E}|_p \in \mathcal{X}$: In such a case, we directly have that $\mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p = \mathsf{Ap}_\delta(\mathcal{E}|_p\Sigma) = \mathsf{Ap}_\delta(\mathcal{E}\Sigma|_p)$. Thus $t = \mathcal{E}\Sigma|_p$ since $names(t) \cap img(\delta) = \emptyset$. Moreover, $\mathcal{E}|_p \in \mathcal{X}$ implies $\mathcal{E}|_p$ does not contain tag_A-tagged term.

Inductive case $\mathsf{root}(\mathcal{E}|_p) = \langle\rangle$: In such a case, $\mathcal{E}|_p = \langle \mathcal{E}_1, \mathcal{E}_2\rangle$. Thus Definition 32 and $\mathsf{Ap}_\delta(t) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p$ imply that there exists t_1, t_2 such that $t = \langle t_1, t_2\rangle$ and $\mathsf{Ap}_\delta(t_i) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_{p\cdot i}$ for $i = 1, 2$. Therefore, by our inductive hypothesis, we deduce that for $i = 1, 2$, $\mathcal{E}|_{p\cdot i}$ does not contain tag_A-tagged term and $t_i = \mathcal{E}\Sigma|_{p\cdot i}$. Since $\mathsf{root}(\mathcal{E}|_p) = \langle\rangle$, we can conclude that $\mathcal{E}|_p$ does not contain tag_A-tagged term and $t = \mathcal{E}\Sigma|_p$

Inductive case $\mathsf{root}(\mathcal{E}|_p) \neq \langle\rangle$: Otherwise, since $\mathcal{E}$ is a fully tag_A-tagged encapsulation, we deduce that $\mathcal{E}|_p = \mathsf{f}(\langle \mathsf{a}, \mathcal{E}_1\rangle, \mathcal{E}_2, \ldots, \mathcal{E}_n)$ for some $\mathsf{a} \in \mathsf{tag}_A$ and some $\mathsf{f} \in \mathcal{F}$. Thus Definition 32 and $\mathsf{Ap}_\delta(t) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_p$ imply that there exists $t_1, \ldots, t_n$ such that $t = \mathsf{f}(\langle \mathsf{a}, t_1\rangle, t_2, \ldots, t_n)$, $\mathsf{Ap}_\delta(t_1) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_{p\cdot 1\cdot 2}$ and for all $i \in \{2, \ldots, n\}$, $\mathsf{Ap}_\delta(t_i) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)|_{p\cdot i}$. By our inductive hypothesis, we deduce that $t_1 = \mathcal{E}\Sigma|_{p\cdot 1\cdot 2}$ and for all $i \in \{2, \ldots, n\}$, $t_i = \mathcal{E}\Sigma|_{p\cdot i}$. Thus we deduce that $t = \mathcal{E}\Sigma|_p$. But we know

that δ is a tag_A-mapping of $[\mathcal{E}\Sigma]$ and $\mathcal{E}\Sigma|_p$ is tag_A-tagged term. Hence by Definition 32, $\mathsf{Ap}_\delta(t) \in \mathcal{N}_D$ which contradicts $t = \mathsf{f}(\langle \mathsf{a}, t_1\rangle, t_2, \ldots, t_n)$. Hence the case $\mathsf{root}(\mathcal{E}|_p) \neq \langle\rangle$ is impossible. ◂

We can now define how we transform an executed frame Φ through a tag_A-mapping of Φ.

▸ **Definition 36.** Let $\mathcal{S}$ be a set of tag_A-encapsulations allowing authentic, confidential and secure channels. Let Φ be a frame. Let D, N, H be three disjoint sets such that Φ is an executed frame for $\mathcal{S}$ and $\mathsf{D} \cup \mathsf{N} \cup \mathsf{H}$. Let δ be a tag_A-mapping of Φ. We define the transformation of Φ by δ, D,N and H, denoted $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)$, recursively on $|\Phi|$ as follows:

- if $|\Phi| = 0$ then $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)$ is the empty frame
- if $\Phi = \Phi' \cdot [u]$ with $|\Phi| \notin \mathsf{D} \cup \mathsf{N} \cup \mathsf{H}$ then $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi') \cdot [\mathsf{Ap}_\delta(u)]$
- if $\Phi = \Phi' \cdot [u]$ with $|\Phi| \in \mathsf{D}$ then $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}-|\Phi|,\mathsf{N}}(\Phi') \cdot [\mathsf{Ap}_\delta(t^i)]$;
- if $\Phi = \Phi' \cdot [u]$ with $|\Phi| \in \mathsf{N}$ then $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}-|\Phi|}(\Phi')$.
- if $\Phi = \Phi' \cdot [u]$ with $|\Phi| \in \mathsf{H}$ and $(\mathcal{E}_{|\Phi|}, \ell_{|\Phi|}, S_{|\Phi|})$ is an encapsulation allowing authentic channels then $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = \mathsf{Tr}^{\mathsf{H}-|\Phi|,\delta}_{\mathsf{D},\mathsf{N}}(\Phi') \cdot [\mathsf{Ap}_\delta(t^i)]$;
- else $\Phi = \Phi' \cdot [u]$ and $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = \mathsf{Tr}^{\mathsf{H}-|\Phi|,\delta}_{\mathsf{D},\mathsf{N}}(\Phi')$.

▸ **Lemma 37.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $I = \mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let δ be a tag_A-mapping of Φ. Assume that Φ is an executed frame for $\mathcal{S}$ and I. We have that for all $t \in dom(\delta)$, if $t\delta \in names(\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)) \cup \bigcup_{i\in I} names(\mathsf{Ap}_\delta(\Sigma_i))$ then $\Phi \vdash t$.*

Proof. Let us denote $\Phi = [u_1; \ldots; u_n]$ and $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = [v_1; \ldots; v_m]$. Let $t \in dom(\delta)$ such that $t\delta \in names(\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)) \cup \bigcup_{i\in I} names(\mathsf{Ap}_\delta(\Sigma_i))$. If $t\delta \in names(\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi))$ then there exists $j \in \{1, \ldots, m\}$ such that $t\delta \in names(v_j)$. Following Definition 36, we deduce that there exists $j \leq i$ such that $i \notin \mathsf{N}$ and:

- either $i \notin \mathsf{D} \cup \mathsf{H}$, $v_j = \mathsf{Ap}_\delta(u_i)$ and so $t \in st(u_i)$
- or $i \in \mathsf{D} \cup \mathsf{H}$, $v_j = \mathsf{Ap}_\delta(\mathsf{t}_{\mathcal{E}_i}\Sigma_i)$ and so $t \in st(\mathsf{t}_{\mathcal{E}_i}\Sigma_i) \subseteq st(\Sigma_i)$.

If $t\delta \in \bigcup_{i\in I} names(\mathsf{Ap}_\delta(\Sigma_i))$ then $t \in st(\Sigma_i)$. Thus, we deduce that either $t \in \bigcup_{i\notin I} st(u_i) \cup \bigcup_{i\in I} st(\Sigma_i)$. Consider $i \notin I$ (resp. $i \in I$) such that $t \in st(u_i)$ (resp. $t \in st(\Sigma_i)$). By Definition 28, since t is a tag_A-term, we deduce that either $[u_1; \ldots; u_{i-1}] \vdash t$ or there exist $t' \in st(u_i)$ (resp. $t' \in st(\Sigma)$) and $k < i$ such that $t \in st(t')$ and $t', t \in st(\mathcal{E}_k\Sigma_k) \setminus st(img(\Sigma_k))$ and $[u_1; \ldots; u_{i-1}] \vdash t'$.

In the former case, the result trivially holds. In the latter case, by Lemma 34, we know that $t' = C[w_1, \ldots, w_{n'}]$ where C is a context built on $\{\langle\,\rangle\} \cup \mathcal{F}_{cst}$ and for all $w_r \in \{1, \ldots, n'\}$, w_r is either a tag_A-term from $dom(\delta)$ or $w_r \in \mathcal{T}(\mathcal{F}_{key} \cup \mathcal{F}_{cst}, img(\Sigma))$. But we know that $t\delta \in names(\mathsf{Ap}_\delta(u_i))$ (resp. $t\delta \in names(\mathsf{Ap}_\delta(\Sigma_i))$) and $t' \in st(u_i)$ (resp. $t' \in st(img(\Sigma_i))$) and $t \in st(t')$. Thus by Definition 32, we deduce that there exists $r \in \{1, \ldots, n'\}$ such that $w_r = t$. Since $[u_1; \ldots; u_{i-1}] \vdash t'$ and C is built on $\{\langle\,\rangle\} \cup \mathcal{F}_{cst}$, we deduce that $[u_1; \ldots; u_{i-1}] \vdash t$ and so the result holds. ◂

Given a set $S \subseteq \mathbb{N}$, given $i \in \mathbb{N}$, we denote by $S|_i$ the set $\{j \in S \mid j < i\}$.

C.3 Deducibility link between composed and abstract frame

▸ **Definition 38.** Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $\mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let δ be a tag_A-mapping of Φ. We say that Φ *is a well formed frame for $\mathcal{S}$,* D, N *and* H if the following properties hold:

- Φ is an executed frame for $\mathcal{S}$ and $\mathsf{D} \cup \mathsf{N} \cup \mathsf{H}$.
- for all $i \in \mathsf{D}$, $\Phi \vdash t^i$.

- for all $i \in \mathsf{N}$, $\Phi \nvdash t^i$.
- for all $i \in \mathsf{H}$, for all $v \in \mathsf{X}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \nvdash v$
- for all $i \in \mathsf{H}$, for all $v \in \mathsf{F}_i\Sigma_i$, $\mathsf{Tr}^{\mathsf{H}|_i,\delta}_{\mathsf{D}|_i,\mathsf{N}|_i}(\Phi) \vdash v$.

▶ **Lemma 39.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $I = \mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let δ be a tag_A-mapping of Φ. Assume that Φ is a well formed frame for $\mathcal{S}$, D, N and H. Let $A = \{a \in img(\delta) \mid u \in dom(\delta), u\delta = a, \Phi \vdash u\}$. For all $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$, if $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash t$ and $names(t) \cap (img(\delta) \setminus A) = \emptyset$ then:*

- *if there exists $t' \in \mathcal{T}(\mathcal{F}, \mathcal{N})$ such that $names(t') \cap img(\delta) = \emptyset$ and $\mathsf{Ap}_\delta(t') = t$ then $\Phi \vdash t'$.*
- *if there exist $i \in I$, a position p of $\mathcal{E}_i$ such that $t = \mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)|_p$ then $\Phi \vdash \mathcal{E}_i\Sigma_i|_p$.*

Proof. Consider a minimal proof P of $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash t$. Let us denote $\Phi = [u_1; \ldots; u_N]$ and $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) = [v_1; \ldots; v_M]$. We prove the result by induction on $\mathcal{M}(P)$.

Base case $\mathcal{M}(P) = (0, 1)$: In such a case, we have that $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$. Assume first that $t \notin img(\delta)$. In such a case, since $names(\Phi) \cap img(\delta) = \emptyset$, it implies for all $i \in I$, for all position p of $\mathcal{E}_i$, $t \neq \mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)$. On other hand, $t \in \mathcal{N}_D \cup \mathcal{F}_{cst}$ and $t \notin img(\delta)$ also imply that $t = \mathsf{Ap}_\delta(t)$ and $names(t) \cap img(\delta) = \emptyset$. Hence $\Phi \vdash t$.

Assume now that $t \in img(\delta)$ then there exists t' such that $t = \mathsf{Ap}_\delta(t')$. Moreover, we know by hypothesis that $names(t) \cap (img(\delta) \setminus A) = \emptyset$ hence $t \in A$ which allows us to deduce that $\Phi \vdash t'$. Lastly, if there exists $i \in I$, a position p of $\mathcal{E}_i$ such that $t = \mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)$ then by Lemma 35, we deduce that $t' = \mathcal{E}_i\Sigma_i|_p$. Hence the result holds since $\Phi \vdash t'$.

Base case $\mathcal{M}(P) = (i, 1)$: In such a case, we deduce that either $t = v_i$ or there exists $k \in I$ such that $t = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)$.

Consider first the case $t = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)$ and there exists $j \in I$ and a position p of $\mathcal{E}_j$ such that $t = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_p$. Thus we have $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k) = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_p$. By Definition 5, we know that there exists $C[\_]$ built on $\{\langle\ \rangle\} \cup \mathcal{F}_{cst}$ and terms $u_1, \ldots, u_n$ such that $\mathcal{E}_j|_p = C[u_1, \ldots, u_n]$ and for all $r \in \{1, \ldots, n\}$, either $u_r \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ or u_r is a tag_A-tagged term. Moreover, with $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k) = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_p$, we deduce that $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k) = C[u_1\mathsf{Ap}_\delta(\Sigma_j), \ldots, u_n\mathsf{Ap}_\delta(\Sigma_j)]$. For all $r \in \{1, \ldots, n\}$, we do a case analysis on u_r and on its position q in C.

- Case $u_r \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ and q is a position of $\mathcal{E}_k$ different from variable: In such a case, we deduce that $u_r\mathsf{Ap}_\delta(\Sigma_j) = \mathsf{Ap}_\delta(u_r\Sigma_j)$ and so $\mathsf{Ap}_\delta(u_r\Sigma_j) = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_q$. But q being a position of $\mathcal{E}_k$ implies, by Lemma 35, that $u_r\Sigma_j = \mathcal{E}_k\Sigma_k|_q$. Since $C[\_]$ built on $\{\langle\ \rangle\} \cup \mathcal{F}_{cst}$ $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k) = C[u_1\mathsf{Ap}_\delta(\Sigma_j), \ldots, u_n\mathsf{Ap}_\delta(\Sigma_j)]$ and q is a position of $\mathcal{E}_k$, we deduce that for all prefix q' of q, $\mathsf{root}(\mathcal{E}_k\Sigma_k|_{q'}) = \langle\ \rangle$ and so $[\mathcal{E}_k\Sigma_k] \vdash \mathcal{E}_k\Sigma_k|_q$. Since $\mathcal{E}_k\Sigma_k \in \Phi$ and $\mathcal{E}_k\Sigma_k|_q = u_r\Sigma_j$, we deduce that $\Phi \vdash u_r\Sigma_j$.
- Case $u_r \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ and q is not a position of $\mathcal{E}_k$ different from variable: Once again, we have $u_r\mathsf{Ap}_\delta(\Sigma_j) = \mathsf{Ap}_\delta(u_r\Sigma_j)$. However, q not being a position of $\mathcal{E}_k$ implies that there exists $y \in dom(\Sigma_k)$ and a prefix q' of q such that $\mathsf{Ap}_\delta(y\Sigma_k) = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_{p\cdot q'}$ and $p \cdot q'$ is a position of $\mathcal{E}_j$. By Lemma 35, we deduce that $y\Sigma_k = \mathcal{E}_j\Sigma_j|_{p\cdot q'}$. Similarly to the previous case, we deduce that all prefix q'' of q', $\mathsf{root}(\mathcal{E}_k\Sigma_k|_{q''}) = \langle\ \rangle$ and so $[\mathcal{E}_k\Sigma_k] \vdash y\Sigma_k = \mathcal{E}_j\Sigma_j|_{p\cdot q'}$. But $u_r\Sigma_j$ is deducible from $\mathcal{E}_j\Sigma_j|_{p\cdot q'}$ hence we can conclude that $\Phi \vdash u_r\Sigma_j$.
- Case u_r is a tag_A-tagged term and q is not a position of $\mathcal{E}_k$ different from variable: Since q is not a position of $\mathcal{E}_k$, then there exists $y \in dom(\Sigma_k)$ and a prefix q' of q such that $\mathsf{Ap}_\delta(y\Sigma_k) = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_{p\cdot q'}$. But by Lemma 35, it would imply that $\mathcal{E}_j|_{p\cdot q'}$ does not contain tag_A-tagged term which is a contradiction with u_r being a tag_A-tagged term. Therefore, this case is impossible.
- Case u_r is a tag_A-tagged term and q is a position of $\mathcal{E}_k$ different from variable: In such a case, $\mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_{p\cdot q} = u_r\mathsf{Ap}_\delta(\Sigma_j) = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_q$ implies that $\mathcal{E}_k|_q$ is also a tag_A-tagged term.

By Property 2 of Definition 7, we deduce that $img(mgu(\mathcal{E}_j|_{p\cdot q}, \mathcal{E}_k|_q))) \subseteq \mathcal{X}$. Thus for all position q', if $\mathcal{E}_j|_{p\cdot q\cdot q'} \in \mathcal{X}$ then $\mathcal{E}_k|_{q\cdot q'} \in \mathcal{X}$ and $\mathcal{E}_j|_{p\cdot q\cdot q'}\mathsf{Ap}_\delta(\Sigma_j) = \mathcal{E}_k|_{q\cdot q'}\mathsf{Ap}_\delta(\Sigma_k)$ which implies $\mathcal{E}_j|_{p\cdot q\cdot q'}\Sigma_j = \mathcal{E}_k|_{q\cdot q'}\Sigma_k$. Therefore, we deduce that $\mathcal{E}_j\Sigma_j|_{p\cdot q} = \mathcal{E}_k\Sigma_k|_q$. But $\mathcal{E}_k\Sigma_k|_q$ is deducible from $\mathcal{E}_k\Sigma_k$ hence so is $u_r\Sigma_j$.

This allows us to conclude that $\Phi \vdash \mathcal{E}_j|_p\Sigma_j$.

Consider now the case $t = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)$ and there exists t' such that $names(t') \cap img(\delta) = \emptyset$ and $\mathsf{Ap}_\delta(t') = t$. By Lemma 35, we deduce that $t' = \mathcal{E}_k\Sigma_k$ and so we directly have that $\Phi \vdash t'$.

Consider now the case $t = v_i$ and there exists $j \in I$, a position p of $\mathcal{E}_j$ such that $t = \mathcal{E}_j\mathsf{Ap}_|(\Sigma_j)_p$. By Definition 36, we know that there exists t' such that $names(t') \cap img(\delta) = \emptyset$ and $\mathsf{Ap}_\delta(t') = v_i$. Hence we have that $\mathcal{E}_j\Sigma_j|_p = t'$. By showing that $\Phi \vdash t'$, the result would thus yield. Therefore, we focus on proving that $\Phi \vdash t'$ which coincides with the last case.

By Definition 36, we know that there exists $j \in \{1, \ldots, n\}$ such that $i \leq j$ and $j \notin \mathsf{N}$ and:

- either $j \notin \mathsf{D} \cup \mathsf{H}$ and $t = \mathsf{Ap}_\delta(u_j)$. In such a case, since $names(u_j, t) \cap img(\delta) = \emptyset$ then $t' = u_j$. Hence we directly have that $\Phi \vdash t'$.
- or $j \in \mathsf{D}$ and $v_i = \mathsf{Ap}_\delta(\mathsf{t}_{\mathcal{E}_j}\Sigma_j)$. Since $names(\mathsf{t}_{\mathcal{E}_j}\Sigma_j, t') \cap img(\delta) = \emptyset$, we have that $\mathsf{t}_{\mathcal{E}_j}\Sigma_j = t$. But by hypothesis, we already know that $\Phi \vdash \mathsf{t}_{\mathcal{E}_j}\Sigma_j$ hence the result holds.
- or $j \in \mathsf{H}$, $(\mathcal{E}_j, \ell_j, S_j)$ is an encapsulation allows authentic channels and $v_i = \mathsf{Ap}_\delta(\mathsf{t}_{\mathcal{E}_j}\Sigma_j)$. Once again, since $names(\mathsf{t}_{\mathcal{E}_j}\Sigma_j, t') \cap img(\delta) = \emptyset$, we deduce that $\mathsf{t}_{\mathcal{E}_j}\Sigma_j = t'$. Moreover, we know by hypothesis the frame is well formed hence by Definition 38, we have that for all $v \in \mathsf{F}_j\mathsf{Ap}_\delta(\Sigma_j)$, $\mathsf{Tr}^{\mathsf{H}|_j,\delta}_{\mathsf{D}|_j,\mathsf{N}|_j}(\Phi) \vdash v$. Following Definition 36, if we denote by P' the proof of $\mathsf{Tr}^{\mathsf{H}|_j,\delta}_{\mathsf{D}|_j,\mathsf{N}|_j}(\Phi) \vdash v$, we obtain that $\mathcal{M}(P') < (i, 1)$. But by Definition 5, we know that each element of F_j is of the form $\mathsf{f}(y)$ where $\mathsf{f} \in \mathcal{F}_{key}$ and $y \in \mathcal{X}$. Hence, we deduce that for all $v' \in \mathsf{F}_j\Sigma_j$, there exists $v \in \mathsf{F}_j\mathsf{Ap}_\delta(\Sigma_j)$ such that $\mathsf{Ap}_\delta(v') = v$. Therefore it implies that for all $v' \in \mathsf{F}_j\Sigma_j$, $\mathsf{Tr}^{\mathsf{H}|_j,\delta}_{\mathsf{D}|_j,\mathsf{N}|_j}(\Phi) \vdash_{P'} \mathsf{Ap}_\delta(v')$ with $\mathcal{M}(P') < (i, 1)$. By applying our inductive hypothesis, we deduce that for all $v' \in \mathsf{F}_j\Sigma_j$, $\Phi \vdash v'$. Therefore, by Property 3 of Definition 7, we deduce that $\Phi \vdash \mathsf{t}_{\mathcal{E}_j}\Sigma_j$ and so $\Phi \vdash t'$.

Inductive case $\mathcal{M}(P) > (i, j)$: Assume first that the last rule of P is a composition rule. In such a case, $t = \mathsf{f}(t_1, \ldots, t_n)$ for some terms $t_1, \ldots, t_n$ and for all $k \in \{1, \ldots, n\}$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)\cdot[\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash t_k$. If there exists t' such that $\mathsf{Ap}_\delta(t') = t$ then by Definition 32, we deduce that $t == \mathsf{f}(\mathsf{Ap}_\delta(t_1), \ldots, \mathsf{Ap}_\delta(t_r))$ for some $t'_1, \ldots, t'_r$ such that $t' = \mathsf{f}(t'_1, \ldots, t'_r)$ and so for all $k \in \{1, \ldots, n\}$, $\mathsf{Ap}_\delta(t'_k) = t_k$. Thus we can apply our inductive hypothesis on all $t'_1, \ldots, t'_n$ and deduce that for all $k \in \{1, \ldots, n\}$, $\Phi \vdash t'_k$ which allows us to conclude that $\Phi \vdash t'$

On the other hand, if there exists $\ell \in I$ and a position p of $\mathcal{E}_\ell$ such that $t = \mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_p$ then either $\mathcal{E}_\ell|_p \in \mathcal{X}$ or for all $k \in \{1, \ldots, n\}$, $t_k = \mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_{p\cdot k}$ with $p \cdot k$ a position of $\mathcal{E}_\ell$. In the former case, we deduce that there exists $x \in \Sigma_\ell$ such that $t = \mathsf{Ap}_\delta(x\Sigma_\ell)$. Therefore, we apply the same reasoning as above. In the latter case, we can apply our inductive hypothesis on all $t_1, \ldots, t_k$ and so we deduce that for all $k \in \{1, \ldots, n\}$, $\Phi \vdash \mathcal{E}_\ell\Sigma_\ell|_{p\cdot k}$ which allows us to conclude.

Assume now that the last rule of P is a decomposition rule. Therefore, there exists $x \in \mathcal{X}$, $u'_1, \ldots, u'_n, v'_1, \ldots, v'_m \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$, a substitution σ and some proofs $P', P_1, \ldots, P_k$ such that:

- $t = x\sigma$
- $vars(v'_1, \ldots, v'_m) \subseteq \{u'_1, \ldots, u'_n\}$; and
- $P = \mathsf{ir}(P', P_1, \ldots, P_m)$; and
- $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)\cdot[\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash_{P'} \mathsf{f}(x, u'_1, \ldots, u'_n)\sigma$ and for all $k \in \{1, \ldots, m\}$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)\cdot[\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash_{P_k} v'_k\sigma$.

Moreover, by minimality of P, we deduce that there exists $i' \leq i$ such that $\mathsf{f}(x, u'_1, \ldots, u'_\ell)\sigma$ is subterm of either $v_{i'}$ or $\mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell)$ for some $\ell \in I$. We do case analysis on these two cases.

Case $\mathsf{f}(x, u'_1, \ldots, u'_\ell)\sigma \in st(v_{i'})$: By Definition 36, we know that there exists $k \in \{1, \ldots, N\}$ such that $i' \leq k$ and $k \notin \mathsf{N}$ and:

- either $k \notin \mathsf{D} \cup \mathsf{H}$ and $v_i = \mathsf{Ap}_\delta(u_k)$;
- or $k \in \mathsf{D} \cup \mathsf{D}$ and $v_i = \mathsf{Ap}_\delta(\mathsf{t}_{\mathcal{E}_k}\Sigma_k)$.

By Definition 32, it implies that there exists t', t'' subterm of Φ such that $\mathsf{f}(x, u'_1, \ldots, u'_n)\sigma = \mathsf{Ap}_\delta(t'')$ with $t'' = \mathsf{f}(t', w_1, \ldots, w_\ell)$, $\mathsf{Ap}_\delta(t') = t$ and for all $r \in \{1, \ldots, n\}$, $\mathsf{Ap}_\delta(w_r) = u'_r\sigma$. However, since for all $r \in \{1, \ldots, n\}$, $u'_r \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ then it implies that for all $y \in dom(\sigma)$, there exists a term w such that $\mathsf{Ap}_\delta(w) = y\sigma$. Let us define the substitution σ' such that for all $y \in dom(\sigma)$, $y\sigma' = w$ where $\mathsf{Ap}_\delta(w) = y\sigma$. Since we also have that for all $r \in \{1, \ldots, m\}$, $v'_1, \ldots, v'_r \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ then we deduce that for all $r \in \{1, \ldots, k\}$, $\mathsf{Ap}_\delta(v'_r\sigma') = v'_r\sigma$. By applying our inductive hypothesis on $\mathsf{Ap}_\delta(t'')$ and $\mathsf{Ap}_\delta(v'_1\sigma'), \ldots, \mathsf{Ap}_\delta(v'_k\sigma')$, we deduce that $\Phi \vdash t''$ and for all $r \in \{1, \ldots, k\}$, $\Phi \vdash v'_r\sigma'$. Thus it allows us to apply the same decomposition rule and conclude that $\Phi \vdash t'$.

Therefore, we have shown that there exists t' such that $names(t') \cap img(\delta) = \emptyset$, $\mathsf{Ap}_\delta(t') = t$ and $\Phi \vdash t'$. Note that since $names(t') \cap img(\delta) = \emptyset$, if there exists another t'' such that $names(t'') \cap img(\delta) = \emptyset$ and $\mathsf{Ap}_\delta(t'') = t$, then $t'' = t'$. Therefore the result holds. Moreover, if there exists $r \in I$ and a position p of $\mathcal{E}_r$ such that $\mathcal{E}_r\mathsf{Ap}_\delta(\Sigma_r)|_p = t$ then by Lemma 35, we deduce that $\mathcal{E}_r\Sigma_r|_p = t'$ and so $\Phi \vdash \mathcal{E}_r\Sigma_r|_p = t'$ which allows us to conclude.

Case $\mathsf{f}(x, u'_1, \ldots, u'_n)\sigma \in st(\mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell))$ for $\ell \in I$: If there is no position p of $\mathcal{E}_\ell$ different from a variable such that $\mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_p = \mathsf{f}(x, u'_1, \ldots, u'_\ell)\sigma$ then it implies that there exists $x \in \Sigma_\ell$ such that $\mathsf{f}(x, u'_1, \ldots, u'_\ell)\sigma \in \mathsf{Ap}_\delta(x\Sigma_\ell)$. Thus, we can apply the same reasoning as in the case $\mathsf{f}(x, u'_1, \ldots, u'_\ell)\sigma \in st(v_{i'})$ which allows us to conclude.

Let us consider the case where there exists a position p of $\mathcal{E}_\ell$ different from a variable such that $Ec_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_p = \mathsf{f}(x, u'_1, \ldots, u'_\ell)\sigma$. We build a substitution σ' as follows:

By Definition 5, we know that for all $r \in \{1, \ldots, m\}$, if $v'_r \notin \mathcal{X}$ then for all $r' \in \{1, \ldots, n\}$, $vars(u'_{r'}) = vars(v'_r) = \{x\}$ implies $Ec_\ell|_{p\cdot(r'+1)} \in \mathcal{X}$. Thus, we define in such a case $x\sigma'$ such that $u'_{r'}\sigma' = Ec_\ell|_{p\cdot(r'+1)}\Sigma_\ell$. It implies that $u'_r\sigma = \mathsf{Ap}_\delta(u'_r\sigma')$ and $v'_r\sigma = \mathsf{Ap}_\delta(v'_r\sigma')$.

Otherwise, if $v'_r \in \mathcal{X}$ then either there exists r' such that $u'_{r'} = v'_r$ or $u'_{r'} = \mathsf{g}(v'_r)$ for some $\mathsf{g} \in \mathcal{F}_{key}$. In the former, it implies that $v'_r\sigma = \mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_{p\cdot(r'+1)}$ where $p \cdot (r' + 1)$ is a position of $\mathcal{E}_\ell$. Thus we define $u'_{r'}\sigma' = \mathcal{E}_\ell\Sigma_\ell|_{p\cdot(r'+1)}$. In the latter, by Definition 5, we deduce that there exists t' such that $v'_r\sigma = \mathsf{Ap}_\delta(t')$ and so $u'_{r'}\sigma = \mathsf{Ap}_\delta(\mathsf{g}(t'))$. By Lemma 35, we deduce thus that $\mathcal{E}_\ell\Sigma_\ell|_{p\cdot(r'+1)} = \mathsf{g}(t')$ and we define $v'_r\sigma' = t'$.

We can therefore apply our inductive hypothesis on $Ec_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_p, v'_1\sigma, \ldots, v'_m\sigma$ which allows us to deduce that $\Phi \vdash \mathcal{E}_\ell\Sigma_\ell|_p = \mathsf{f}(x\sigma', u'_1\sigma', \ldots, u'_n\sigma')$ and for all $r \in \{1, \ldots, m\}$, $\Phi \vdash v'_r\sigma'$. Thus we can apply the same decomposition rule and obtain that $\Phi \vdash \mathcal{E}_\ell\Sigma_\ell|_{p\cdot 1}$.

Let us conclude by verifying the two hypothesis: if there exists t' such that $\mathsf{Ap}_\delta(t') = t$ then by Lemma 35, we deduce that $t' = \mathcal{E}_\ell\Sigma_\ell|_{p\cdot 1}$ and so the result holds. If there exists $\ell' \in I$ and a position p' of $\mathcal{E}_{\ell'}$ such that $t = \mathcal{E}_{\ell'}\mathsf{Ap}_\delta(\Sigma_{\ell'})|_{p'}$, then we obtain that $\mathcal{E}_{\ell'}\mathsf{Ap}_\delta(\Sigma_{\ell'}) = \mathcal{E}_\ell\mathsf{Ap}_\delta(\Sigma_\ell)|_{p\cdot 1}$ with $\Phi \vdash \mathcal{E}_\ell\Sigma_\ell|_{p\cdot 1}$. Therefore, we can apply the same reasoning as in he base case $\mathcal{M}(P) = (i, 1)$ and $t = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k) = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_p$ with $\Phi \vdash \mathcal{E}_k\Sigma_k$. This allows us to conclude. ◂

▸ **Lemma 40.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $I = \mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let δ be a tag_A-mapping of Φ. Assume that Φ is a well formed frame for $\mathcal{S}$, D, N and H. Let $I' \subseteq I$ such that for all $i \in I'$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash \mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)$. For all $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash t$ implies $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash t$.*

Proof. Let $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$ such that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash t$. We prove the result by induction on $|I'|$.

Base case $|I'| = 0$*:* Trivial.

Inductive case $|I'| > 0$*:* Let $k \in I'$, we do a case analysis on k.

- Case $k \in \mathsf{D}$: By Definition 36, we know that $\mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k) \in \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)$. Thus, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)\cdot[\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash t$ implies that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'\setminus\{k\}} \vdash t$. By our inductive hypothesis on $I' \setminus \{k\}$, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash t$.
- Case $k \in \mathsf{N}$: In such a case, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)\cdot[\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$ implies $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)\cdot[\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$. By Lemma 37, we know that for all names $a \in img(\delta) \cap names(\mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k))$, for all term u, $u \in dom(\delta)$ and $u\delta = a$ implies $\Phi \vdash u$. Thus, if we denote $A = \{a \in img(\delta) \mid u \in dom(\delta), u\delta = a, \Phi \vdash u\}$, we deduce that $names(\mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)) \cap (img(\delta) \setminus A) = \emptyset$. Therefore, by Lemma 39, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I} \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$ implies that $\Phi \vdash \mathsf{t}_{\mathcal{E}_k}\Sigma_k$. This is a contradiction with the fact that Φ is a well formed frame for $\mathcal{S}$, D, N and H. Hence this case is impossible.
- Case $k \in \mathsf{H}$ and $(\mathcal{E}_k, \mathsf{F}_k)$ allows authentic channels: This case is similar to the case $k \in \mathsf{D}$ since $\mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k) \in \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi)$ by Definition 36.
- Case $k \in \mathsf{H}$ and $(\mathcal{E}_k, \mathsf{F}_k)$ does not allow authentic channels: In such a case, $(\mathcal{E}_k, \mathsf{F}_k)$ satisfies Property 4 of Definition 7. Thus, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$ implies that either $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'\setminus\{k\}} \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$ or there exists $x \in \mathsf{X}_{\mathcal{E}_k}$ such that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'\setminus\{k\}} \vdash x\mathsf{Ap}_\delta(\Sigma_k)$. In the latter, by inductive hypothesis on $I \setminus \{k\}$, we would deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash x\mathsf{Ap}_\delta(\Sigma_k)$ which is in contradiction with the fact that Φ is a well formed frame for $\mathcal{S}$, D, N and H. Hence we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'\setminus\{k\}} \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$. By applying our inductive hypothesis on $I' \setminus \{k\}$, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{t}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k)$. Thus, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'} \vdash t$ implies that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)]_{i\in I'\setminus\{k\}} \vdash t$. By our inductive hypothesis on $I' \setminus \{k\}$, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash t$.

◀

▶ **Lemma 41.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $\mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let δ be a tag_A-mapping of Φ. Assume that Φ is a well formed frame for $\mathcal{S}$, D, N and H. Let us denote $I = \mathsf{D} \cup \mathsf{N} \cup \mathsf{H}$. The following two properties hold:*

- *for all terms t, $names(t) \cap img(\delta) = \emptyset$ and $\Phi \vdash t$ imply $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$*
- *for all $i \in I$, for all positions p of $\mathcal{E}_i$, if $\Phi \vdash_P \mathcal{E}_i(t^i, s^i_1, \ldots, s^i_{\ell_i})|_p$ then the term $\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)|_p$ is deducible from the frame $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I}$.*

Proof. Let a term t such that $names(t) \cap img(\delta) = \emptyset$ and $\Phi \vdash_P t$. Consider that P is minimal. We will prove both properties by induction on $\mathcal{M}(P)$. In particular, for the second property, we will assume that $t = \mathcal{E}_i\Sigma_i|_p$ for some $i \in I$ and position p of $\mathcal{E}_i$. Let us denote $\Phi = [w_1; \ldots; w_n]$.

Base case $\mathcal{M}(P) = (0, 1)$*:* In such a case, $P = 0$ and so $t \in \mathcal{N}_D$ or $t \in \mathcal{F}_{cst}$. Therefore, we deduce that $\mathsf{Ap}_\delta(t) = t$ and so $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$. Regarding the second property, if there exists $i \in I$ and a position p of $\mathcal{E}_i$ such that $\mathcal{E}_i\Sigma_i|_p = t$ then either $\mathcal{E}_i|_p \in \mathcal{X} \cup \mathcal{F}_{cst}$. In such a case, we deduce that $\mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)|_p = t$ and so the result holds since $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash t$.

Base case $\mathcal{M}(P) = (i, 1)$*:* In such a case, $P = i$ and so $t = w_i$. We do a case analysis whether $i \in I$ or not.

Case $i \notin I$: By Definition 36, we know that there exists $j \leq i$ such that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash_j \mathsf{Ap}_\delta(t)$. Thus the first property directly holds. Regarding the second property, assume that there exists $j \in I$ and

a position p of $\mathcal{E}_j$ such that $t = \mathcal{E}_j\Sigma_j|_p$. By Lemma 34, we know that $\mathcal{E}_j\Sigma_j = C[u_1, \ldots, u_m]$ where $C[\_]$ is a context built on $\{\langle\ \rangle\} \cup \mathcal{F}_{cst}$ and for all $k \in \{1, \ldots, m\}$, u_k is either a tag_A-term of $dom(\delta)$ or $u_k \in vars(\mathcal{E}_i)\Sigma_i$ or a term of the form $\mathsf{f}(v)$ for some $\mathsf{f} \in \mathcal{F}_{key}$ and $v \in \mathsf{X}_{\mathcal{E}_i}\Sigma_i \cup \mathcal{F}_{cst}$. We know that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$. Hence, for all $k \in \{1, \ldots, m\}$, if u_k is not a tag_A-term of $dom(\delta)$, it implies that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(u_k)$. If u_k is a tag_A-term of $dom(\delta)$, we know by Definition 28 that there exists P' such that $\mathcal{M}(P') < (i, 1)$ and $\Phi \vdash_{P'} u_k$. Moreover, there exists a position p' of $\mathcal{E}_j$ such that $u_k = \mathcal{E}_j\Sigma_j|_{p'}$ hence we can apply our inductive hypothesis on it which means that by combining both results, the result holds.

Case $i \in I$: In such case, by Lemma 34, we know that $\mathcal{E}_i\Sigma_i = C[u_1, \ldots, u_m]$ where $C[\_]$ is a context built on $\{\langle\ \rangle\} \cup \mathcal{F}_{cst}$ and for all $k \in \{1, \ldots, m\}$, u_k is either a tag_A-term of $dom(\delta)$ or $u_i \in vars(\mathcal{E}_i)\Sigma_i$ or a term of the form $\mathsf{f}(v)$ for some $\mathsf{f} \in \mathcal{F}_{key}$ and $v \in \mathsf{X}_{\mathcal{E}_i}\Sigma_i \cup \mathcal{F}_{cst}$. Since $t = w_i$, it implies that for all $k \in \{1, \ldots, m\}$, $\Phi \vdash u_k$. But by Definition 7 and in particular by Property 1 using the empty frame, we can deduce that for all $k \in \{1, \ldots, m\}$, u_k is either a tag_A-term of $dom(\delta)$ or $u_k \in \{\mathsf{t}_{\mathcal{E}_i}\Sigma_i\} \cup \mathcal{T}(\mathcal{F}_{key} \cup \mathcal{F}_{cst}, \emptyset)$. Moreover, by Property 4 of Definition 7 and by Definition 38, we deduce that u_k can only be either a tag_A-term of $dom(\delta)$ or $u_k \in \mathcal{T}(\mathcal{F}_{key} \cup \mathcal{F}_{cst}, \emptyset)$ when $i \in \mathsf{D}$ or when $(\mathcal{E}_i, \mathsf{F}_i)$ does not allow authentic channels.

Furthermore, if $(\mathcal{E}_i, \mathsf{F}_i)$ is an encapsulation allowing authentic channels, we know that by Definition 36 that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)$. Since by Lemma 34, we have $\mathsf{Ap}_\delta(t) = C[\mathsf{Ap}_\delta(u_1), \ldots, \mathsf{Ap}_\delta(u_m)]$ and $\mathsf{Ap}_\delta(u_1) \ldots, \mathsf{Ap}_\delta(u_m) \in \mathcal{N}_D \cup \{\mathsf{t}_{\mathcal{E}_i}\mathsf{Ap}_\delta(\Sigma_i)\} \cup \mathcal{T}(\mathcal{F}_{key} \cup \mathcal{F}_{cst}, \emptyset)$, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$.

Let us focus now on the second property. Assume that there exists $j \in I$ and a position p of $\mathcal{E}_j$ such that $t = \mathcal{E}_j\Sigma_j|_p$. If $\mathcal{E}_j|_p \in \mathcal{X}$ then we have that $\mathsf{Ap}_\delta(t) = \mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_p$. But we already proved that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$ hence the result directly holds. If $\mathcal{E}_j|_p \notin \mathcal{X}$ then in such a case, $\mathcal{E}_j\Sigma_j|_p = \mathcal{E}_i\Sigma_i$ implies that $\mathcal{E}_j|_p$ is unifiable with $\mathcal{E}_i$. Let us consider the $\mathcal{E}_j|_p$. We know by definition that $\mathcal{E}_j|_p = C'[r_1, \ldots, r_\ell]$ where C' is built on pair for all $k \in \{1, \ldots, \ell\}$, $r_k \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$ or r_k is a tag_A-term. In the former, since $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(r_k\Sigma_j)$. In the latter, if q is the position of r_k in $\mathcal{E}_j$ and q is also a position of $\mathcal{E}_i$ different from a variable, then by Property 2 of Definition 5, we deduce that $\mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j)|_{p\cdot q} = \mathcal{E}_i\mathsf{Ap}_\delta(\Sigma_i)|_q$. Therefore, we have that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash r_k\mathsf{Ap}_\delta(\Sigma_j)$. Otherwise by Definition 28, we know that there exists a proof Q such that $\mathcal{M}(Q) < (i, 1)$ and $\Phi \vdash_Q r_k\Sigma_j$. Thus we can apply our inductive hypothesis on it which allows us to deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash r_k\mathsf{Ap}_\delta(\Sigma_j)$. And so the result holds.

Inductive case $\mathcal{M}(P) = (i, j)$ with $j > 1$: Let us do a case analysis on the last rule of the proof.

Assume first that the last rule of the proof is an f-composition rule. Therefore, there exists $t_1, \ldots, t_m$ and ir such that $t = \mathsf{f}(t_1, \ldots, t_m)$, $P = \mathsf{ir}(P_1, \ldots, P_m)$ and for all $i \in \{1, \ldots, m\}$, $\Phi \vdash_{P_i} t_i$. If $t \in dom(\delta)$ then $\mathsf{Ap}_\delta(t) \in \mathcal{N}_D$ and so we directly have $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$. Else $t \notin dom(\delta)$ and since for all $i \in \{1, \ldots, m\}$, $\mathcal{M}(P_i) < \mathcal{M}(P)$ then by inductive hypothesis on all the t_i, we deduce that for all $i \in \{1, \ldots, m\}$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t_i)$. Moreover, thanks to $t \notin dom(\delta)$, we know that $\mathsf{Ap}_\delta(t) = \mathsf{f}(\mathsf{Ap}_\delta(t_1), \ldots, \mathsf{Ap}_\delta(t_m))$. Hence we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$. Consider now that there exists $r \in I$ and a position p of $\mathcal{E}_r$ such that $t = \mathcal{E}_r\Sigma_r$. If $\mathcal{E}_r|_p \in \mathcal{X}$ then $\mathsf{Ap}_\delta(t) = \mathcal{E}_r\mathsf{Ap}_\delta(\Sigma_r)|_p$. Therefore, we directly have that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$ as previously shown and so the result holds. If $\mathcal{E}_r|_p \notin \mathcal{X}$ then we can apply our inductive hypothesis on all t_k with position $p \cdot k$ and so the result also holds.

Assume now that the last rule is an f-decomposition. Therefore, there exists $x \in \mathcal{X}, u_1, \ldots, u_m, v_1, \ldots, v_k \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$, a substitution σ and some proofs $P', P_1, \ldots, P_k$ such that:

- $t = x\sigma$
- $vars(v_1, \ldots, v_k) \subseteq \{u_1, \ldots, u_m\}$; and
- $P = \mathsf{ir}(P', P_1, \ldots, P_k)$; and

- $\Phi \vdash_{P'} \mathsf{f}(x, u_1, \ldots, u_m)\sigma$ and for all $r \in \{1, \ldots, k\}$, $\Phi \vdash_{P_r} v_r\sigma$.

Moreover, by minimality of P, we know that there exists $i' \leq i$ such that P is a successive sequence of applications of decomposition rules on $w_{i'}$. We do a case analysis on $\mathsf{f}(x, u_1, \ldots, u_m)\sigma$ and i'.

Case $\mathsf{f}(x, u_1, \ldots, u_n)\sigma \in dom(\delta)$ *and* $i' \notin I$*:* Since P is a successive sequence of applications of decomposition rules on $w_{i'}$, we deduce that there exists a position p such that $w_{i'}|_p = \mathsf{f}(x, u_1, \ldots, u_n)\sigma$ and $(i', 1) \leq \mathcal{M}(P') < (i, j)$. But by Definition 28, we know that either $[w_1; \ldots; w_{i'-1}] \vdash w_{i'}|_p$ or else $p = p' \cdot a \cdot p''$ such that $[w_1; \ldots; w_{i'-1}] \vdash w_{i'}|_{p' \cdot a}$. Moreover, P being a successive sequence of applications of decomposition rules on $w_{i'}$ implies that there exists $P'' \in st(P)$ such that $(i', 1) \leq \mathcal{M}(P'')$ and $\Phi \vdash_{P''} w_{i'}|_{p' \cdot a}$. Since we already know that $[w_1; \ldots; w_{i'-1}] \vdash w_{i'}|_{p' \cdot a}$ then there is a contradiction with the fact that P is minimal.

Case $\mathsf{f}(x, u_1, \ldots, u_n)\sigma \in dom(\delta)$*,* $i' \in I$ *and* $\mathsf{f}(x, u_1, \ldots, u_n\sigma) \in st(\Sigma_{i'})$*:* Similar to the previous case, meaning that we obtain a contradiction with the fact that P is minimal.

Case $t \in dom(\delta)$ *and either* $i' \notin I$ *or* $t \in st(\Sigma_{i'})$*:* Similar to the previous case.

For the next cases, we need to look at different cases depending on the property we prove. Moreover, we have to switch from one property to the other depending on the case.

Property 1 *Case* $\mathsf{f}(x, u_1, \ldots, u_n)\sigma \notin dom(\delta)$*:* In such a case, we have $\mathsf{Ap}_\delta(\mathsf{f}(x\sigma, u_1\sigma, \ldots, u_n\sigma)) = \mathsf{f}(\mathsf{Ap}_\delta(x\sigma), \mathsf{Ap}_\delta(u_1\sigma), \ldots, \mathsf{Ap}_\delta(u_m\sigma))$. By our inductive hypothesis, we deduce $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{f}(\mathsf{Ap}_\delta(x\sigma), \mathsf{Ap}_\delta(u_1\sigma), \ldots, \mathsf{Ap}_\delta(u_m\sigma))$ and for all $i \in \{1, \ldots, k\}$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(v_i\sigma)$. But $u_1\sigma, \ldots, u_m\sigma, v_1\sigma, \ldots, v_k\sigma \in \mathcal{T}(\mathcal{F}_{key}, \mathcal{X})$, hence we deduce that for all i, $\mathsf{Ap}_\delta(u_i\sigma) = u_i\mathsf{Ap}_\sigma(\sigma)$ and $\mathsf{Ap}_\delta(v_i\sigma) = v_i\mathsf{Ap}_\sigma(\sigma)$. This allows us to deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(x\sigma)$.

Property 2 *Case for all* $k \in I$ *and all positions* p *of* $\mathcal{E}_k$*,* $\mathcal{E}_k\Sigma_k|_p \neq \mathsf{f}(x, u_1, \ldots, u_n)\sigma$ *:* In such a case, we deduce that $i' \notin I$. However, we know that there exists $k \in I$ and a position p of $\mathcal{E}_k$ such that $\mathcal{E}_k\Sigma_k|_p = t$. Therefore, by Lemma 34, we deduce that $t = C[u'_1, \ldots, u'_{n'}]$ such that for all $r \in \{1, \ldots, n'\}$, either u'_r is a tag_A-term or $u'_r \in vars(\mathcal{E}_k)\Sigma_k$ or u'_r is of the form $\mathsf{f}(v)$ for some $\mathsf{f} \in \mathcal{F}_{key}$ and some $v \in \mathsf{X}_{\mathcal{E}_k}\Sigma_k \cup \mathcal{F}_{cst}$. From the previous case, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$ and so for all $r \in \{1, \ldots, n'\}$, $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(u'_r)$. But by Lemma 34, we know that $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_p = C[v'_1, \ldots, v'_{n'}]$ such that for all $r \in r \in \{1, \ldots, n'\}$, if u'_r is not a tag_A-term then $v'_r = \mathsf{Ap}_\delta(u'_r)$. Moreover, if u'_r is a tag_A-term then by Definition 28, we know $[w_1; \ldots; w_{i'-1}] \vdash u'_r$. We also know that there exists a position p' of $\mathcal{E}_k$ such that $\mathcal{E}_k\Sigma_k|_{p'} = u'_r$. Hence we can apply our inductive hypothesis on u'_r and obtain that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k \in I} \vdash \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_{p'}$. By combining the two cases (u'_r being a tag_A-term or not), we deduce that the term $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_p$ is deducible from $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k \in I}$.

Property 2 *Case there exists* $k \in I$ *and a position* p *of* $\mathcal{E}_k$ *such that* $\mathcal{E}_k\Sigma_k|_p = \mathsf{f}(x, u_1, \ldots, u_n)\sigma$*:* We can apply our inductive hypothesis on $\mathsf{f}(x, u_1, \ldots, u_n)\sigma$ which allows us to deduce that $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_p$ is deducible from $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k \in I}$. We show that we can apply the same rule ir. Let us look at the terms $v_1, \ldots, v_{m'}$ and construct a new substitution σ'. For all $r \in \{1, \ldots, m'\}$, by Definition 5

- either $v_r = \mathsf{g}(x)$ for some $x \in \mathcal{X}$, $\mathsf{g} \in \mathcal{F}_{key}$ and for all $r' \in \{1, \ldots, n\}$, if $x \in vars(u_{r'})$ then $u_{r'}\sigma \in vars(\mathcal{E}_k)\Sigma_k \cup \mathcal{F}_{cst}$. Therefore, for all $r' \in \{1, \ldots, n\}$, if $x \in vars(u_{r'})$ then $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_{p \cdot (r'+1)} = \mathsf{Ap}_\delta(u_{r'}\sigma)$. Therefore, we define $x\sigma' = \mathsf{Ap}_\delta(x\sigma)$. Note that in such a case, $\mathsf{Ap}_\delta(v_r\sigma) = v_r\sigma'$. Moreover, since $\Phi \vdash_{P_r} v_r\sigma$ then by our inductive hypothesis, we have that $\mathsf{Tr}^{\delta,\Phi}_{I_D,I_H}(\vdash)\mathsf{Ap}_\delta(v_r\sigma)$ and so $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash v_r\sigma'$.
- or $v_r \in X$ and for all $r' \in \{1, \ldots, n\}$, if $v_r \in vars(u_{r'})$ then $u_{r'}\sigma = v_r\sigma$. In such a case, we define $v_r\sigma' = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_{p \cdot (r'+1)}$. Note that since $\Phi \vdash_{P_r} v_r\sigma$, we can apply our inductive hypothesis on $v_r\sigma$ and the position $p \cdot (r' + 1)$ which indicates that the term $v_r\sigma'$ is deducible from the frame $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k \in I}$.

- or $v_r \in X$ and there exists $r' \in \{1, \ldots, n)$ such that $v_r \in vars(u_{r'})$ and $u_{r'}\sigma = \mathsf{g}(v)$ with $\mathsf{g} \in \mathcal{F}_{key}$ and $v \in \mathsf{X}_{\mathcal{E}_k}\Sigma_k \cup \mathcal{F}_{cst}$. In such a case, we define $v_r\sigma' = \mathsf{Ap}_\delta(v)$. Similarly to the first case, we deduce $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash v_r\sigma'$.

This allows us to conclude that $\mathsf{f}(x, u_1, \ldots, u_m)\sigma' = \mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_p$ and $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash v_r\sigma'$ for all $r \in \{1, \ldots, m'\}$. Therefore, we conclude that $\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)|_{p\cdot 1}$ is deducible from $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I}$.

Property 1 *Case* $\mathsf{f}(x, u_1, \ldots, u_n)\sigma \in dom(\delta)$*:* Considering all the different cases we went through, it implies that $i' \in I$ and there exists a position p of $\mathcal{E}_{i'}$ such that $\mathcal{E}_{i'}\Sigma_{i'}|_p = t$. Therefore, by Lemma 34, we know that $t = C[d_1, \ldots, d_k]$ where C is a context built on $\{\langle\_\rangle\} \cup \mathcal{F}_{cst}$ and for all $r \in \{1, \ldots, k\}$, d_r is either a tag_A-term or $d_r \in vars(\mathcal{E}_{i'})\Sigma_{i'}$ or $d_r = \mathsf{g}(v)$ with $\mathsf{g} \in \mathcal{F}_{key}$ or $v \in \mathsf{X}_{\mathcal{E}_{i'}}\Sigma_{i'} \cup \mathcal{F}_{cst}$. By applying Property 2 on t, we deduce that for all $r \in \{1, \ldots, k\}$, if d_r is not a tag_A-term then $\mathsf{Ap}_\delta(d_r)$ is deducible from $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I}$. Let us consider the different cases:

- if $d_r \in \mathcal{T}(\mathcal{F}_{key} \cup \mathcal{F}_{cst}, \mathsf{X}_{\mathcal{E}_{i'}}\Sigma_{i'})$ then by Property 1 of Definition 7 and Lemma 40, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(d_r)$.
- if $d_r = \mathsf{t}_{\mathcal{E}_{i'}}\Sigma_{i'}$ and $i' \in \mathsf{N}$ then this case is in fact impossible since $\Phi \vdash t$ implies $\Phi \vdash t^{i'}$ which is a contradiction with Definition 38.
- if $d_r = \mathsf{t}_{\mathcal{E}_{i'}}\Sigma_{i'}$ and $i' \in \mathsf{D}$ or $(\mathcal{E}_{i'}, \mathsf{F}_{i'})$ is an encapsulation allowing authentic channels, then by Definition 36, we know that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(d_r)$
- if $d_r = \mathsf{t}_{\mathcal{E}_{i'}}\Sigma_{i'}$ and $i' \in \mathsf{H}$ and $(\mathcal{E}_{i'}, \mathsf{F}_{i'})$ is an not encapsulation allowing authentic channels, then by Property 4 of Definition 7 and Lemma 40, either $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(d_r)$ or there exists $x \in \mathsf{X}_{\mathcal{E}_{i'}}$ such that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash x\mathsf{Ap}_\delta(\Sigma_{i'})$. But the latter case contradicts our initial hypothesis given in Definition 38. Therefore, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(d_r)$.

Lastly, for all $r \in \{1, \ldots, k\}$, if d_r is a tag_A-term then $\mathsf{Ap}_\delta(d_r) \in \mathcal{N}_D$ and so we trivially have that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash d_r$. This allows us to conclude that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash C[\mathsf{Ap}_\delta(d_1), \ldots, \mathsf{Ap}_\delta(d_k)]$ and so $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(t)$. ◀

▶ **Lemma 42.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $\mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let δ be a tag_A-mapping of Φ. Assume that Φ is a well formed frame for $\mathcal{S}$, D, N and H. Let us denote $I = \mathsf{D} \cup \mathsf{N} \cup \mathsf{H}$.*

For all $(\mathcal{E}, \mathsf{F}) \in \mathcal{S}$, for all substitution Σ, for all position p of $\mathcal{E}$, if $\Phi \vdash \mathcal{E}\Sigma|_p$ then there exists a context $C[\_, \ldots, \_]$ and some terms $u_1, \ldots, u_n$ such that $\mathcal{E}\Sigma|_p = C[u_1, \ldots, u_n]$ and for all $i \in \{1, \ldots, n\}$, $\Phi \vdash u_i$ and if q is position of u_i in $\mathcal{E}\Sigma|_p$ then $p \cdot q$ is a position of $\mathcal{E}$ and

- *either $\mathcal{E}|_{p\cdot q} \in \mathcal{X}$;*
- *or $\mathcal{E}|_{p\cdot q} = \mathsf{f}(x)$ with $\mathsf{f} \in \mathcal{F}_{key}$ and $x \in \mathsf{X}_{\mathcal{E}} \cup \mathcal{F}_{cst}$;*
- *or $\mathcal{E}|_{p\cdot q}$ is a tag_A-tagged term and there exists $k \in I$ and a position q' of $\mathcal{E}_k$ such that $\mathcal{E}_k|_{q'} \notin \mathcal{X}$ and $u_i = \mathcal{E}_k\Sigma_k|_{q'}$.*

Proof. Let us denote $\Phi = [w_1; \ldots; w_{|\Phi|}]$. Consider the minimal proof P such that $\Phi \vdash_P \mathcal{E}\Sigma|_p$. We prove the result by induction on $\mathcal{M}(P)$.

Base case $P = (0, 1)$: In such a case, $\mathcal{E}\Sigma|_p \in \mathcal{N}_D \cup \mathcal{F}_{cst}$. Thus it necessarily implies that $\mathcal{E}|_p \in \mathcal{X}$. Hence the result holds with $C = \_$.

Inductive case $P = (i, j)$ and the last rule of P is a decomposition: In such a case, we deduce that there exists $k \leq i$ such that $\mathcal{E}\Sigma|_p \in st(w_k)$.

By Definition 5, we know that there exists a context $C[\_, \ldots, \_]$ built on $\{\langle\ \rangle\} \cup \mathcal{F}_{cst}$ and some terms $v_1, \ldots, v_n$ such that $\mathcal{E}|_p = C[v_1, \ldots, v_n]$ and for all $i \in \{1, \ldots, n\}$, either v_i is a tag_A-term or

$v_i \in \mathcal{X}$ or $v_i = \mathsf{f}(x)$ for some $\mathsf{f} \in \mathcal{F}_{key}$ and $x \in \mathsf{X}_{\mathcal{E}} \cup \mathcal{F}_{cst}$. Therefore, for all $i \in \{1, \ldots, n\}$, thanks to the fact that $C[\_, \ldots, \_]$ is built on $\{\langle\ \rangle\} \cup \mathcal{F}_{cst}$, we deduce that $\Phi \vdash v_i\Sigma$. If v_i is a tag_A-tagged term then we do a small case analysis on k.

Case $k \in I$ and there exists a position q' of $\mathcal{E}_k$ such that $\mathcal{E}_k|'_q \notin \mathcal{X}$ and $v_i = \mathcal{E}_k\Sigma_k|_{q'}$: Trivial

Case $k \notin I$ or $\mathcal{E}_k|_{q'} \in \mathcal{X}$: In such a case, $v_i\Sigma$ being a tag_A-term implies thanks to Definition 28, we deduce that either there exist $k' \in I$ and a position q'' of $\mathcal{E}_{k'}$ different from a variable such that $v_i\Sigma = \mathcal{E}_{k'}|_{q''}\Sigma_k$ or $[w_1; \ldots; w_{k-1}] \vdash v_i\Sigma$. In the former, the result directly holds. In the latter, we can apply our inductive hypothesis on $v_i\Sigma$ since $k - 1 < i$ which allows us to deduce the existence of a context C_i and terms $u^i_1, \ldots, u^i_{n_i}$ satisfying the correct properties. In such a case, we can directly conclude with the context $C[C_1, \ldots, C_n]$ where $C_k = \_$ in the case where u_k is not a tag_A-tagged term else the context C_k obtained through the inductive hypothesis.

Inductive case $P = (i, j)$ with the last rule of P being a composition: In such a case, $\mathcal{E}\Sigma|_p = \mathsf{f}(t_1, \ldots, t_n)$ where for all $k \in \{1, \ldots, n\}$, $\Phi \vdash t_k$. If $\mathcal{E}|_p \in \mathcal{X}$ the result directly holds. Else for all $k \in \{1, \ldots, n\}$, $p \cdot k$ is a position $\mathcal{E}$. Therefore, we can apply our inductive hypothesis on t_k and so we deduce the existence of a context C_k and terms $u^k_1, \ldots, u^k_{m_k}$ satisfying the correct properties. In such a case, we can directly conclude with the context $\mathsf{f}[C_1, \ldots, C_n]$ and the terms $u^1_1, \ldots, u^1_{n_1}, \ldots, u^n_{m_n}$. ◀

▶ **Lemma 43.** *Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a frame. Let D, N, H be three disjoint sets such that $I = \mathsf{D} \cup \mathsf{N} \cup \mathsf{H} \subseteq \{1, \ldots, |\Phi|\}$. Let $(\mathcal{E}, \mathsf{F}) \in \mathcal{S}$. Let Σ be a ground substitution. Let δ be a tag_A-mapping of $\Phi \cdot [\mathcal{E}\Sigma]$. Assume that Φ is a well formed frame for $\mathcal{S}$, D, N and H.*

If $\Phi \vdash \mathcal{E}\Sigma$ and $(\mathcal{E}, \mathsf{F})$ allows confidential channels then

- *either there exists $k \in \mathsf{H}$ such that $\mathcal{E}_k \sim \mathcal{E}$ and $\mathcal{E}_k\Sigma_k = \mathcal{E}\Sigma$;*
- *or $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$.*

If $\Phi \vdash \mathcal{E}\Sigma$; and for all $i \in \mathsf{H}$, either $\mathsf{X}_{\mathcal{E}_i}\Sigma_i = \mathsf{X}_{\mathcal{E}}\Sigma$ or $\mathsf{X}_{\mathcal{E}_i}\Sigma_i \cap \mathsf{X}_{\mathcal{E}}\Sigma = \emptyset$; and $(\mathcal{E}, \mathsf{F})$ does not allow confidential channels then

- *if there exists $k \in \mathsf{H}$ such that $\mathsf{X}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k) = \mathsf{X}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$ then there exist $k \in \mathsf{H}$ such that $\mathcal{E}_k \sim \mathcal{E}$ and $\mathcal{E}_k\Sigma_k = \mathcal{E}\Sigma$;*
- *if for all $k \in \mathsf{H}$, $\mathsf{X}_{\mathcal{E}_k}\mathsf{Ap}_\delta(\Sigma_k) \cap \mathsf{X}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma) = \emptyset$ then $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$.*

Proof. W.l.o.g. consider that the variable of $(\mathcal{E}, \mathsf{F})$ are disjoint from the variables of $(\mathcal{E}_k, \mathsf{F}_k)$ for all $k \in I$. By Lemma 42, we know that there exists a context $C[\_, \ldots, \_]$ and some terms $u_1, \ldots, u_n$ such that $\mathcal{E}\Sigma = C[u_1, \ldots, u_n]$ and for all $i \in \{1, \ldots, n\}$, $\Phi \vdash u_i$ if p is position of u_i in $\mathcal{E}\Sigma$ then p is a position of $\mathcal{E}$ and

- either $\mathcal{E}|_p \in \mathcal{X}$;
- or $\mathcal{E}|_p = \mathsf{f}(x)$ with $\mathsf{f} \in \mathcal{F}_{key}$ and $x \in \mathsf{X}_{\mathcal{E}} \cup \mathcal{F}_{cst}$;
- or $\mathcal{E}|_p$ is a tag_A-tagged term and there exists $k \in I$ and a position q of $\mathcal{E}_k$ such that $\mathcal{E}_k|_q \notin \mathcal{X}$ and $u_i = \mathcal{E}_k\Sigma_k|_q$.

Let us first prove that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash \mathcal{E}\mathsf{Ap}_\delta(\Sigma)$. Let $i \in \{1, \ldots, n\}$. Let us denote by p is position of u_i in $\mathcal{E}\Sigma$. If $\mathcal{E}|_p \in \mathcal{X}$ then by Lemma 41, $\Phi \vdash u_i$ implies that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{Ap}_\delta(\mathcal{E}|_p\Sigma) = \mathcal{E}|_p\mathsf{Ap}_\delta(\Sigma)$. Similarly, if $\mathcal{E}|_p = \mathsf{f}(x)$ with $\mathsf{f} \in \mathcal{F}_{key}$ and $x \in \mathsf{X}_{\mathcal{E}} \cup \mathcal{F}_{cst}$ then we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathcal{E}|_p\mathsf{Ap}_\delta(\Sigma)$.

Otherwise $\mathcal{E}|_p$ is a tag_A-tagged term and there exist $k \in I$ and a position q of $\mathcal{E}_k$ such that $\mathcal{E}_k|_q \notin \mathcal{X}$ and $u_i = \mathcal{E}_k\Sigma_k|_q$. But $\mathcal{E}|_p\Sigma = \mathcal{E}_k|_q\Sigma_k$ implies that $\mathcal{E}|_p$ and $\mathcal{E}_k|_q$ are unifiable. Therefore, by Property 2 of Definition 7, we deduce that $img(mgu(\mathcal{E}_k|_q, \mathcal{E}|_p)) \subseteq X$. Therefore, $\mathcal{E}_k|_q\Sigma_k = \mathcal{E}|_p\Sigma$ implies $\mathcal{E}_k|_q\mathsf{Ap}_\delta(\Sigma_k) = \mathcal{E}|_p\mathsf{Ap}_\delta(\Sigma)$. But we know that $\Phi \vdash \mathcal{E}|_p\Sigma$ and so $\Phi \vdash \mathcal{E}_k|_q\Sigma_k$. Hence by

Lemma 41, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash \mathcal{E}_k|_q\mathsf{Ap}_\delta(\Sigma_k)$. This allows us to deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash \mathcal{E}|_p\mathsf{Ap}_\delta(\Sigma)$. This allows us to conclude that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \cdot [\mathcal{E}_k\mathsf{Ap}_\delta(\Sigma_k)]_{k\in I} \vdash \mathcal{E}\mathsf{Ap}_\delta(\Sigma)$.

By applying Property 5 of Definition 7 and Lemma 40, we deduce that if $(\mathcal{E}, \mathsf{F})$ allows confidential channels then:

- either there exists $j \in I$ such that $\mathcal{E}_j \sim \mathcal{E}$ and $\mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)$; If $j \in \mathsf{H}$ then the result holds. Else $j \in \mathsf{N} \cup \mathsf{D}$. But in both cases, $\mathsf{t}_{\mathcal{E}_j}\mathsf{Ap}_\delta(\Sigma_j) \in \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi)$. Hence we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$.
- or $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$ which implies $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$

This allows us to conclude when $(\mathcal{E}, \mathsf{F})$ allows confidential channels.

By applying Property 6 of Definition 7 and Lemma 40, we deduce that if $(\mathcal{E}, \mathsf{F})$ does not allow confidential channels then:

- either there exists $j \in I$ such that $\mathcal{E}_j \sim \mathcal{E}$ and $\mathcal{E}_j\mathsf{Ap}_\delta(\Sigma_j) = \mathcal{E}\mathsf{Ap}_\delta(\Sigma)$. Hence the result holds.
- or there exists $x \in \mathsf{X}_{\mathcal{E}}$ such that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash x\mathsf{Ap}_\delta(\Sigma)$ and $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$. Hence the result holds
- or there exists $j \in I$, $y \in \mathsf{X}_{\mathcal{E}} \cap \mathsf{X}_{\mathcal{E}_j}$, $x \in \mathsf{X}_{\mathcal{E}}$ such that $y\Sigma = y\Sigma_j$, $\mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma) = \mathsf{t}_{\mathcal{E}_j}\mathsf{Ap}_\delta(\Sigma_j)$ and $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash x\mathsf{Ap}_\delta(\Sigma)$. But by hypothesis, we know that for all $i \in \mathsf{H}$, either $\mathsf{X}_{\mathcal{E}_i}\Sigma_i = \mathsf{X}_{\mathcal{E}}\Sigma$ or $\mathsf{X}_{\mathcal{E}_i}\Sigma_i \cap \mathsf{X}_{\mathcal{E}}\Sigma = \emptyset$. In such a case, by Definition 38 and since $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D},\mathsf{N}}(\Phi) \vdash x\mathsf{Ap}_\delta(\Sigma)$, we deduce that $j \notin \mathsf{H}$. Therefore, by definition of $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi)$, we deduce that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi) \vdash \mathsf{t}_{\mathcal{E}}\mathsf{Ap}_\delta(\Sigma)$.

◀

C.4 From the composed protocol to the abstract protocol (New)

The events added to a process P when created an annotation $\tilde{P}$ under a mapping ρ (Definition 9) contain sufficient information to express when $\tilde{P}$ is a secure channel establishment protocol (Definition 16). However, the channels in the events of $\tilde{P}$ are public since they are not restricted by any new operator. For the proof of Theorem 17, we need to link these public channels with the abstract channels actually restricted in the context of Q. Therefore, we consider below new events $\tilde{\mathsf{ev}}_1, \ldots, \tilde{\mathsf{ev}}_n, \ldots$ of arity 5 in which the last elements will be used to "store" the abstract channels actually restricted in the context of Q. Let us denote $\tilde{\mathsf{Ev}} = \{\tilde{\mathsf{ev}}_1, \ldots, \tilde{\mathsf{ev}}_n, \ldots\}$. Considering these new events, we also define a notion of process *secure* similar to Definition 16.

▶ **Definition 44.** Let P be a closed process. We say that P is secure when for all $(P, \emptyset, \emptyset, \overset{)}{\Rightarrow} e_1 \cdot \ldots \cdot e_m(P', \Phi', \mu', \theta')$, for all $i \in \{1, \ldots, m\}$, if $e_i = ev(c, ta, (s_1, \ldots, s_\ell), (u_1, \ldots, u_q), d)$ such that $ev \in \tilde{\mathsf{Ev}}$ and all agents in ta are honest then for all $k \in \{1, \ldots, \ell\}$, $\Phi' \nvdash s_k$ and for all $k \in \{1, \ldots, q\}$, $\Phi' \vdash u_k$. Moreover, for all $j \in \{1, \ldots, m\}$, if $e_j = ev'(c', ta', (s'_1, \ldots, s'_{\ell'}), (u'_1, \ldots, u'_{q'}), d')$ for some channel c', d', some tuple ta' of agents and some tuples $(s'_1, \ldots, s'_{\ell'})$ and $(u'_1, \ldots, u'_{q'})$ of terms then

- either $ta \neq ta'$ or $c \neq c'$ or $ev = ev'$ implies $\forall k \in \{1, \ldots, \ell\}, \forall k' \in \{1, \ldots, \ell'\}$, $s_k \neq s'_{k'}$
- or one of the two following properties is satisfied :
  - $(s_1, \ldots, s_\ell) = (s'_1, \ldots, s'_{\ell'})$ and $(u_1, \ldots, u_q) = (u'_1, \ldots, u'_{q'})$.
  - $\forall k \in \{1, \ldots, \ell\}, \forall k' \in \{1, \ldots, \ell'\}$, $s_k \neq s'_{k'}$.

Note that the definition is almost identical of Definition 16. The only difference is that we consider events from $\tilde{\mathsf{Ev}}$ instead of the events $\{\mathsf{ev}_1, \ldots, \mathsf{ev}_n, \ldots\}$.

We also define a property on the trace linking the two channels of the events from $\tilde{\mathsf{Ev}}$.

▶ **Definition 45.** Let P be a closed process. We say that an execution $(P, \emptyset, \emptyset, \emptyset) \xrightarrow{e_1 \cdot \ldots \cdot e_m} (P', \Phi', \mu', \theta')$ is *well formed* if for all $i, j \in \{1, \ldots, m\}$, if $e_i = ev(c, ta, ts, tp, d)$, $e_j = ev'(c, ta, ts, tp, d')$, $ev, ev' \in \tilde{\mathsf{Ev}}$, the agents of ta are honest, $ev \neq ev'$ and $d \neq d'$ for some $c, ta, ts, tp, d, d', ev, ev'$ then

- either there exists $i' < i$ such that $e_{i'} = ev(c, ta, ts, tp, d'')$ for some $d'' \neq d$;
- or there exists $j' < j$ such that $e_{j'} = ev'(c, tq, ts, tp, d'')$ for some $d'' \neq d'$.

▶ **Lemma 46.** *Let S be a set of channels. Let $P = C[R_1, \ldots, R_n]$ be a closed process such that:*

- *for all $i \in \{1, \ldots, n\}$, if $c \in S$ appears in R_i then it can only be inside an unique event $\tilde{\mathsf{ev}}_i(d, ta, ts, tp, c)$ for some d, ta, ts, tp where $A \in ta$, A is the agent of R_i and $\mathsf{new}_{ta}\ c$ is in C.*
- *there exists a bijective mapping γ from S to fresh channels for all $i \in \{1, \ldots, n\}$, for all $\tilde{\mathsf{ev}}_i(d, ta, ts, tp, c)$ in R_i, $c\gamma = d$.*

For all $(P, \emptyset, \emptyset, \emptyset) \overset{tr}{\Rightarrow} (Q, \Phi, \mu, \theta)$, there exists Q', θ', tr' such that $(P, \emptyset, \emptyset, \emptyset) \overset{tr'}{\Rightarrow} (Q', \Phi, \mu, \theta')$ and this configuration is well formed.

Proof. Consider $(P, \emptyset, \emptyset, \emptyset) \xrightarrow{e_1 \cdot \ldots \cdot e_n} (Q, \Phi, \mu, \theta)$. Since the channels of S only appear in the events of P, the choices of channels during the execution of the rule New-c do not affect the execution of the trace other than the value of the channels in $e_1 \cdot \ldots \cdot e_n$. Let us create a partition $\uplus_{j=1}^{m} I_j$ of $\{1, \ldots, n\}$ such that for all $j \in \{1, \ldots, m\}$, for all $k, k' \in I_j$, the fifth argument of e'_k and $e'_{k'}$ have been instantiated by the same execution of the rule New-c, for all $k \in I_j$ for all $k \in I_{j'}$ with $j \neq j'$, the fifth argument of e'_k and $e'_{k'}$ have been instantiated by two different execution of the rule New-c. This allows us to build recursively θ' on the m, i.e. on the order of execution of the rule New-c. Typically, when two events $(ev_i(d, ta, ts, tp, c)$ and $ev_j(d', ta', ts', tp', c'))$ of the same partition, meaning $i \neq j$ satisfy $ta = ta'$ and $d = d'$ then we select the same channels if $(ts, tp) = (ts', tp')$. ◀

Let us denote by T_t the set of tuples of terms.

▶ **Definition 47.** Let $\mathcal{S}$ be a set of tag_A-encapsulations. We say that P is an *initial process* when for all instances $\mathsf{out}_A(c, u)$ (resp. $\mathsf{in}_A(c, u)$) in P,

- either u is a fully tag_B-tagged term;
- or $c = c_{pub}$ and $u = \mathcal{E}\Sigma$ for some fully tag_B-tagged substitution Σ and some encapsulation $(\mathcal{E}, \mathsf{F}) \in \mathcal{S}$.

Let us denote by $channels_{O/I}(P)$ the set of channels appearing in an output or input of P. Note that $channels(P) \setminus channels_{O/I}(P)$ is not necessary empty since a channel c can be declared by $\mathsf{new}\ c$ in P but never used in an output or input.

▶ **Definition 48.** Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be an executed ground frame for $\mathcal{S}$ and some I. Let P be an initial process. Let α be a mapping from $\mathcal{S} \times T_t$ to Ch. We say that α is *a mapping of channels for P (resp. Φ)* when $img(\alpha) \cap channels_{O/I}(P) = \emptyset$ and for all $(\mathcal{E}, \mathsf{F}) \in \mathcal{S}$, for all substitution Σ, if $\mathcal{E}\Sigma$ is in P (resp. for all $i \in I$, if $\mathcal{E}\Sigma = \mathcal{E}_i\Sigma_i$) then there exists $c \in Ch$ such that $((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha = c$ and if $(\mathcal{E}, \mathsf{F})$ allows authentic (resp. confidential, secure) channels then $c \in Ch_a \cup Ch_p$ (resp. $Ch_c \cup Ch_p$, $Ch_s \cup Ch_p$).

We define the transformed process of P w.r.t. α, denoted $\mathsf{Tr}_\alpha(P)$, as the process P where we replace:

- all instances $\mathsf{out}_{A_i}(c_{pub}, \mathcal{E}\Sigma)$ by $\mathsf{out}_{A_i}(c, \mathsf{t}_{\mathcal{E}}\Sigma)$
- all instances $\mathsf{in}_{A_i}(c_{pub}, \mathcal{E}\Sigma)$ by $\mathsf{in}_{A_i}(c, \mathsf{t}_{\mathcal{E}}\Sigma)$

when $((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha = c$ for some Σ and F.

▶ **Definition 49.** Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be an ground executed frame for some set I. Let P be an initial process. Let α (resp. β) be a mapping of channels for P (resp. Φ). Let σ a substitution of closed terms. Let tr be a sequence of closed events. We say that P,Φ, α, β, tr and σ have conforming events if

1. for all $i \in I$, there exist c, d, ta, k such that $((\mathcal{E}_i, \mathsf{F}_i), \mathsf{X}_{\mathcal{E}_i}\Sigma_i)\beta = d$, $\tilde{\mathsf{ev}}_k(c, ta, \mathsf{X}_{\mathcal{E}_i}\Sigma_i, \mathsf{F}_i\Sigma_i, d) \in tr$ and $d \notin Ch_p$ is equivalent to all agents in ta are honest; and
2. for all roles $R = r_1.\ldots.r_n$ of P, for all $i \in \{1, \ldots, n\}$, if $r_i = \mathsf{out}_A(c_{pub}, \mathcal{E}\Sigma)$ (resp. $r_i = \mathsf{in}_A(c_{pub}, \mathcal{E}\Sigma)$) for some agent A, some substitution Σ and some encapsulation $(\mathcal{E}, \mathsf{F}) \in \mathcal{S}$ then there exists c, d, ta such that $((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha = d$ and:
   - either there exist $j < i$ and $ev \in \tilde{\mathsf{Ev}}$ such that $r_j = \mathsf{event}_A(ev(c, ta, \mathsf{X}_{\mathcal{E}}\Sigma, \mathsf{F}\Sigma), d)$;
   - or $ev(c, ta, \mathsf{X}_{\mathcal{E}}\Sigma\sigma, \mathsf{F}\Sigma\sigma, d) \in tr$ and $d \notin Ch_p$ is equivalent to all agents in ta are honest.

When tr and Φ are the empty sequence and σ is the identity, we say that P, α have conforming events.

▶ **Definition 50.** Let $\mathcal{S}$ be a set of tag_A-encapsulations. Let Φ be a well formed frame for $\mathcal{S}$ and some D, N and H. Let β be a mapping of channels for Φ. We define $\mu(\Phi, \beta)$ as a mapping from channels to sets of terms such that:

- $dom(\mu(\Phi, \beta)) = \{c \notin Ch_p \mid i \in \mathsf{H} \wedge ((\mathcal{E}_i, \mathsf{F}_i), \mathsf{X}_{\mathcal{E}_i}\Sigma_i)\beta = c\}$; and
- $\forall c \in dom(\mu(\Phi, \beta)), c\mu(\Phi, \beta) = \{\mathsf{Ap}_\delta(\mathsf{t}_{\mathcal{E}_i}\Sigma_i) \mid i \in \mathsf{H} \wedge ((\mathcal{E}_i, \mathsf{F}_i), \mathsf{X}_{\mathcal{E}_i}\Sigma_i)\beta = c\}$.

▶ **Lemma 51.** *Let $\mathcal{S}$ be a set of tag_A-tagged encapsulations allowing authentic, confidential and secure channels. Let P_0 be a closed initial process. Let α_0 be a mapping of channels for P_0. Assume that P_0,α_0 have conforming events. Assume that $(\mathsf{Tr}_\alpha(P_0), \emptyset, \emptyset, \emptyset)$ is secure. For all well-formed execution $(P_0, \emptyset, \emptyset, \emptyset) \overset{tr}{\Rightarrow}_\sigma (P, \Phi, \mu, \theta)$, there exists an initial process Q, a mapping of channels α (resp. β) for Q (resp. Φ), and η, δ, D, N and H such that:*

- *$Q\sigma = P$; and*
- *$\eta\sigma = \mu$ and η only contains fully tag_B-terms; and*
- *Q, Φ, α, β, tr and σ have conforming events; and*
- *Φ is a well formed frame for $\mathcal{S}$, D, N and H; and*
- *σ is an executed substitution for Φ; and*
- *δ is a tag_A-mapping of Φ and σ; and*
- *$(\mathsf{Tr}_\alpha(P_0), \emptyset, \emptyset, \emptyset) \overset{\mathsf{Ap}_\delta(tr)}{\Longrightarrow}_{\mathsf{Ap}_\delta(\sigma)} (\mathsf{Tr}_\alpha(Q)\mathsf{Ap}_\delta(\sigma), \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi), \eta\mathsf{Ap}_\delta(\sigma) \circ \mu(\Phi, \beta), \theta)$*

Proof. We do the proof by induction on the size of the trace $(P_0, \emptyset, id) \overset{tr}{\Rightarrow}_\sigma (P, \Phi, \mu)$:

Base case: The result trivially holds with $Q = P_0$, $\alpha = \alpha_0$, $\beta = id$, $\delta = id$, $\mathsf{D} = \mathsf{N} = \mathsf{H} = \emptyset$.

Inductive step: In such case, we assume that there exist two processes P_1 and P_2, two substitutions σ_1, σ_2, two frames Φ_1, Φ_2 and two mapping μ_1, μ_2 such that $(P_0, \emptyset, id) \overset{tr_1}{\Rightarrow}_{\sigma_1} (P_1, \Phi_1, \mu_1) \overset{e}{\rightarrow}_{\sigma_2} (P_2, \Phi_2, \mu_2)$. By applying our inductive hypothesis on $(P_0, \emptyset, id) \overset{tr_1}{\Rightarrow}_{\sigma_1} (P_1, \Phi_1, \mu_1)$, we deduce that there exist an initial process Q_1, a mapping of channels α_1 (resp. β_1) for Q_1 (resp. Φ_1), and η_1, δ_1, D_1, N_1, H_1 such that:

- $Q_1\sigma_1 = P_1$; and
- $\eta_1\sigma_1 = \mu_1$ and η_1 only contains fully tag_B-terms; and
- Q_1, Φ_1, α_1, β_1, tr_1 and σ_1 have conforming events; and
- Φ_1 is a well formed frame for $\mathcal{S}$, D_1, N_1 and H_1; and

- σ_1 is an executed substitution for Φ_1; and
- δ_1 is a tag_A-mapping of Φ_1 and σ_1; and
- $(\mathsf{Tr}_\alpha(P_0), \emptyset, id) \xRightarrow{\mathsf{Ap}_{\delta_1}(tr_1)}_{\sigma'_1} (\mathsf{Tr}_{\alpha_1}(Q_1)\sigma'_1, \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1), \eta_1\sigma'_1 \circ \mu(\Phi_1,\beta_1))$ with $\sigma'_1 = \mathsf{Ap}_{\delta_1}(\sigma_1)$.

We show the existence of an initial process Q_2, a mapping of channels α_2 (resp. β_2) for Q_2 (resp. Φ_2), and η_2, δ_2, D_2, N_2 and H_2 satisfying the result with (P_2, Φ_2, μ_2) by case analysis on the rule applying in $(P_1, \Phi_1, \mu_1) \xrightarrow{e}_{\sigma_2} (P_2, \Phi_2, \mu_2)$.

Rule Out: In such a case, $Q_1 = Q \mid \mathsf{out}_A(c,u).R_A$, $P_2 = Q\sigma_1 \mid R_A\sigma_1$, $\sigma_2 = \sigma_1$, $\Phi_2 = \Phi_1 \cdot [u\sigma_1]$ if $c \in Ch_p \cup Ch_a$ else $\Phi_2 = \Phi_1$, and $\mu_2 = \mathsf{rect}(c, u\sigma_1, \mu_1)$ if $c \notin Ch_p$ else $\mu_2 = \mu_1$. Let us first define $Q_2 = Q \mid R_A$. This allows us to deduce that $Q_2\sigma_2 = P_2$. Let us also define $tr_2 = tr_1$ and $\alpha_2 = \alpha_1$. Therefore, we deduce that $\mathsf{Tr}_{\alpha_2}(Q_2) = \mathsf{Tr}_{\alpha_1}(Q_1) \mid \mathsf{Tr}_{\alpha_1}(R_A)$.

By Definition 47, we know that either u is a fully tag_B-tagged term and $c \notin img(\alpha_1) \cup img(\beta_1)$ or $u = \mathcal{E}\Sigma$ and $c = c_{pub} \in Ch_p$ where Σ is a fully tag_B-tagged substitution and $(\mathcal{E}, \mathsf{F})$ is an encapsulation. We do a case analysis:

Case u is a tag_B-tagged term and $c \notin img(\alpha_1) \cup img(\beta_1)$: In such a case, $\mathsf{Tr}_{\alpha_1}(Q_1) = \mathsf{Tr}_{\alpha_1}(Q) \mid \mathsf{out}_A(c,u).\mathsf{Tr}_{\alpha_1}(R_A)$. Since u is a tag_B-tagged term, we deduce that $\mathsf{Ap}_{\delta_1}(u\sigma_1) = u\mathsf{Ap}_{\delta_1}(\sigma_1)$ thus if $\mu_2 = \mathsf{rect}(c, u\sigma_1, \mu_1)$ (when $c \notin Ch_p$) then we can define $\eta_2 = \mathsf{rect}(c, u, \eta_1)$ and obtain that $\mu_2 = \eta_2\sigma_1 = \eta_2\sigma_2$ and $\eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) = \mathsf{rect}(c, u\mathsf{Ap}_{\delta_1}(\sigma_1), \eta_1\mathsf{Ap}_{\delta_1}(\sigma_1))$.

Consider N_2 and D_2 such that $\mathsf{N}_2 \cup \mathsf{D}_2 = \mathsf{N}_1 \cup \mathsf{D}_1$ and such that for all $i \in \mathsf{N}_2$ (resp. D_2), $\Phi_2 \not\vdash t^i$ (resp. $\Phi_2 \vdash t^i$). Consider $\mathsf{H}_2 = \mathsf{H}_1$, $\delta_2 = \delta_1$ and $\beta_2 = \beta_1$. In such a case, if $\Phi_2 = \Phi_1 \cdot [u\sigma_1]$ (when $c \in Ch_p \cup Ch_a$) then we deduce that $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) = \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1) \cdot [\mathsf{Ap}_{\delta_1}(u\sigma_1)] = \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1) \cdot [u\mathsf{Ap}_{\delta_1}(\sigma_1)]$. This allows us to deduce that $\mu(\Phi_2, \beta_2) = \mu(\Phi_1, \beta_1)$ and so:

$$(\mathsf{Tr}_{\alpha_1}(Q_1)\mathsf{Ap}_{\delta_1}(\sigma_1), \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1), \eta_1\mathsf{Ap}_{\delta_1}(\sigma_1) \circ \mu(\Phi_1,\beta_1)) \rightarrow (\mathsf{Tr}_{\alpha_2}(Q_2)\mathsf{Ap}_{\delta_2}(\sigma_2), \mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2), \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_2,\beta_2))$$

Moreover, since $\sigma_2 = \sigma_1$, $tr_1 = tr_2$, $\alpha_2 = \alpha_2$, $\beta_2 = \beta_1$, all outputs and inputs of P_2 are in P_1 and $\mathsf{N}_2 \cup \mathsf{D}_2 \cup \mathsf{H}_2 = \mathsf{N}_1 \cup \mathsf{D}_1 \cup \mathsf{H}_1$, we deduce that $P_2, \Phi_2, \alpha_2, \beta_2, tr_2$ and σ_2 have conforming events. Furthermore, we know that σ_1 is an executed substitution for Φ_1 and u is a tag_B-tagged term. Hence for all subterms of $u\sigma_1$ that are tag_A-tagged term, they are subterm of $img(\sigma_1)$. Hence following Definitions 31 and 38, we deduce that Φ_2 is a well formed frame for $\mathcal{S}$, D_2, N_2 and H_2. We also directly have that σ_2 is an executed substitution for Φ_2 since Φ_1 is included in Φ_2. Lastly, since δ_1 is a tag_A-mapping of Φ_1 and σ_1 then we know that all tag_A-tagged terms in $img(\sigma_1)$ are in $dom(\delta_1)$, thus so do the one in $u\sigma_1$. Hence we deduce that δ_2 is a tag_A-mapping of Φ_2 and σ_2. This allows us to conclude.

Case $u = \mathcal{E}\Sigma$ and $c = c_{pub} \in Ch_p$: In this case, by Definition 49, we deduce that there exists a channel d such that $((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha_1 = d$. Let us show that if $((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma\sigma_1)\beta_1 = d'$ for some channel d' and either $d \notin Ch_p$ or $d' \notin Ch_p$ then $d = d'$. By definition 48, we know that there exists $i \in \mathsf{H}_1 \cup \mathsf{N}_1 \cup \mathsf{D}_1$ such that $(\mathcal{E}_i, \mathsf{F}_i) = (\mathcal{E}, \mathsf{F})$, $\mathsf{X}_{\mathcal{E}_i}\Sigma_i\sigma_1 = \mathsf{X}_{\mathcal{E}}\Sigma\sigma_1$ and $((\mathcal{E}_i, \mathsf{F}_i), \mathsf{X}_{\mathcal{E}_i}\Sigma_i)\beta_1 = d'$. Therefore, by Definition 49, we know that there exists $ev' \in \tilde{\mathsf{Ev}}$, c'_0 and ta' such that $ev'(c'_0, ta', \mathsf{X}_{\mathcal{E}_i}\Sigma_i\sigma_1, \mathsf{F}_i\Sigma_i\sigma_1, d') \in tr_1$ and all agents in ta' are honest is equivalent to $d' \notin Ch_p$. Moreover, with the same definition, we also know that there exists $ev \in \tilde{\mathsf{Ev}}$, c_0 and ta such that $ev(c_0, ta, \mathsf{X}_{\mathcal{E}}\Sigma\sigma_1, \mathsf{F}\Sigma\sigma_1, d) \in tr_1$ and all agents in ta are honest is equivalent to $d \notin Ch_p$. But we know that $(\mathsf{Tr}_\alpha(P_0), \emptyset, id)$ is secure. Hence by our inductive hypothesis on $(\mathsf{Tr}_\alpha(P_0), \emptyset, id)$, if either $d \notin Ch_p$ or $d' \notin Ch_p$ then we deduce that all the agents in either ta or ta' are honest and thus since $\mathsf{X}_{\mathcal{E}_i}\Sigma_i\sigma_1 = \mathsf{X}_{\mathcal{E}}\Sigma\sigma_1$ we obtain by Definition 44 that $t_a = t'_a$, $c_0 = c'_0$ and $ev \neq ev'$. But we also know that the execution $(P_0, \emptyset, id) \overset{tr}{\Rightarrow}_\sigma (P, \Phi, \mu)$ is well formed. Hence by Definition 45, we deduce that $d = d'$. So $\mathsf{X}_{\mathcal{E}_i}\Sigma_i\sigma_1 = \mathsf{X}_{\mathcal{E}}\Sigma\sigma_1$ implies that $d = d'$.

Therefore, let us define $\beta_2 = \beta_1 \circ \{((\mathcal{E}, \mathsf{F}), \mathsf{X}_\mathcal{E}\Sigma\sigma_1) \to d\}$ if $d \notin Ch_p$ or if $((\mathcal{E}, \mathsf{F}), \mathsf{X}_\mathcal{E}\Sigma\sigma_1) \notin dom(\beta_1)$. Otherwise, we define $\beta_2 = \beta_1$.

Moreover, $u = \mathcal{E}\Sigma$ and $c \in Ch_p$ imply $\mathsf{Tr}_{\alpha_1}(Q_1) = \mathsf{Tr}_{\alpha_1}(Q) \mid \mathsf{out}_A(d, \mathsf{t}_\mathcal{E}\Sigma).\mathsf{Tr}_{\alpha_1}(R_A)$, $\Phi_2 = \Phi_1 \cdot [u\sigma_1]$ and $\mu_2 = \mu_1$. Therefore, by defining $\eta_2 = \eta_1$, we have that:

$$(\mathsf{Tr}_{\alpha_1}(Q_1)\mathsf{Ap}_{\delta_1}(\sigma_1), \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1), \eta_1\mathsf{Ap}_{\delta_1}(\sigma_1) \circ \mu(\Phi_1, \beta_1)) \to (\mathsf{Tr}_{\alpha_2}(Q_2)\mathsf{Ap}_{\delta_2}(\sigma_2), \Phi_2', \mu_2')$$

where $\Phi_2' = \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1) \cdot [\mathsf{t}_\mathcal{E}\Sigma\mathsf{Ap}_{\delta_1}(\sigma_1)]$ if $d \in Ch_p \cup Ch_a$, else $\Phi_2' = \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1)$; and where $\mu_2' = \mathsf{rect}(d, \mathsf{t}_\mathcal{E}\Sigma\mathsf{Ap}_{\delta_1}(\sigma_1), \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_1, \beta_1))$ if $d \notin Ch_p$ else $\mu_2' = \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_1, \alpha_1)$. Note that $\mathsf{t}_\mathcal{E}\Sigma$ is a tag_B-tagged term hence $\mathsf{t}_\mathcal{E}\Sigma\mathsf{Ap}_{\delta_1}(\sigma_1) = \mathsf{Ap}_{\delta_1}(\mathsf{t}_\mathcal{E}\Sigma\sigma_1)$. Moreover, we also directly have that σ_2 is an executed substitution for Φ_2 since σ_1 is an executed substitution for Φ_1 and Φ_1 is included in Φ_2. Furthermore, we know that Σ is a fully tag_B-tagged substitution. Hence for all subterms of $\Sigma\sigma_1$ that are tag_A-tagged term, they are subterm of $img(\sigma_1)$. Hence following Definitions 31 and 28, we deduce that Φ_2 is an executed frame for $\mathcal{S}$ and $\mathsf{D}_1 \cup \mathsf{N}_1 \cup \mathsf{H}_1 \cup \{|\Phi_1| + 1\}$. Note that by construction of β_2 and by Definition 49, we also deduce that P_2, Φ_2, α_2, β_2, tr_2 and σ_2 have conforming events. We do a small case analysis on d:

- *Case $d \in Ch_p$:* In such a case, we define $\mathsf{H}_2 = \mathsf{H}_1$ and $\mathsf{D}_2, \mathsf{N}_2$ such that $\mathsf{D}_2 \cup \mathsf{N}_2 = \mathsf{D}_1 \cup \mathsf{N}_1 \cup \{|\Phi_1| + 1\}$ and for all $i \in \mathsf{N}_2$ (resp. D_2), $\Phi_2 \not\vdash \mathsf{t}_{\mathcal{E}_i}\Sigma_i$ (resp. $\Phi_2 \vdash \mathsf{t}_{\mathcal{E}_i}\Sigma_i$). Since $\delta_1 = \delta_2$ and $\sigma_1 = \sigma_2$ then by Definition 36, we deduce that $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) = \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1) \cdot [\mathsf{Ap}_{\delta_2}(\mathsf{t}_\mathcal{E}\Sigma\sigma_2)] = \Phi_2'$. Moreover, since $d \in Ch_p$ then by Definition 50, we deduce that $\mu(\Phi_2, \beta_2) = \mu(\Phi_1, \beta_1)$. Hence we can conclude that $\mu_2' = \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_2, \beta_2)$. Lastly, since $\mathsf{H}_2 = \mathsf{H}_1$ and we already proved that Φ_2 is an executed frame for $\mathcal{S}$ and $\mathsf{D}_2 \cup \mathsf{N}_2 \cup \mathsf{H}_2$, we deduce that Φ_2 is a well formed frame for $\mathcal{S}$, D_2, N_2 and H_2. This allows us to conclude.
- *Case $d \notin Ch_p$:* In such a case, we define $\mathsf{H}_2 = \mathsf{H}_1 \cup \{|\Phi_1| + 1\}$ and D_2, N_2 such that $\mathsf{D}_2 \cup \mathsf{N}_2 = \mathsf{D}_1 \cup \mathsf{N}_1$ and for all $i \in \mathsf{N}_2$ (resp. D_2), $\Phi_2 \not\vdash \mathsf{t}_{\mathcal{E}_i}\Sigma_i$ (resp. $\Phi_2 \vdash \mathsf{t}_{\mathcal{E}_i}\Sigma_i$). By Definition 47, we know that $(\mathcal{E}, \mathsf{F})$ allows authentic (resp. confidential, secure) channels implies $d \in Ch_a$ (resp. Ch_c, Ch_s). Therefore, since $\delta_1 = \delta_2$ and $\sigma_1 = \sigma_2$ then by Definition 36, we deduce that $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) = \Phi_2'$. Let us now focus on μ_2'. We know that $\mu_2' = \mathsf{rect}(d, t\mathsf{Ap}_{\delta_1}(\sigma_1), \eta_2\mathsf{Ap}_{\sigma_2}(\sigma_2) \circ \mu(\Phi_1, \alpha_1))$. But if $d \notin dom(\mu_1)$ then we need to look at $\mu(\Phi_1, \alpha_1)$. Since we defined $\beta_2 = \beta_1 \circ \{((\mathcal{E}, \mathsf{F}), \mathsf{X}_\mathcal{E}\Sigma\sigma_1) \to d\}$, $\Phi_2 = \Phi \cdot [\mathcal{E}\Sigma\sigma]$ and $\mathsf{H}_2 = \mathsf{H}_1 \cup \{|\Phi_1| + 1\}$, we deduce by definition that $\mu(\Phi_2, \beta_2) = \mathsf{rect}(d, \mathsf{t}_\mathcal{E}\Sigma\mathsf{Ap}_{\delta_1}(\sigma), \mu(\Phi_1, \beta_1))$. Since $\mu_1 = \mu_2$, $\delta_2 = \delta_1$ and $dom(\mu_1) \cap img(\beta_2) = \emptyset$, we deduce that $\mathsf{rect}(d, \mathsf{t}_\mathcal{E}\Sigma\mathsf{Ap}_{\delta_1}(\sigma_1), \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_1, \beta_1)) = \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_2, \beta_2) = \mu_2'$.
  It remains to prove that Φ_2 is a well formed frame for $\mathcal{S}$, D_2, N_2 and H_2. We already know that σ_1 is an executed substitution for Φ_1 and Σ does not contain tag_A-tagged term. Therefore, since $\Phi_2 = \Phi_1 \cdot [\mathcal{E}\Sigma\sigma_1]$ then we deduce that Φ_2 is an executed frame for $\mathsf{D}_2 \cup \mathsf{N}_2 \cup \mathsf{H}_2$. Let us prove that for all $v \in \mathsf{X}_\mathcal{E}\Sigma\sigma_1$, $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \not\vdash \mathsf{Ap}_{\delta_2}(v)$ and $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash \mathsf{FAp}_{\delta_2}(\Sigma\sigma_1)$. We know $(\mathsf{Tr}_\alpha(P_0), \emptyset, id) \xRightarrow{\mathsf{Ap}_{\delta_2}(tr_2)}_{\mathsf{Ap}_{\delta_2}(\sigma_2)} (\mathsf{Tr}_{\alpha_2}(Q_2)\mathsf{Ap}_{\delta_2}(\sigma_2), \mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2), \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2) \circ \mu(\Phi_2, \beta_2))$, $(\mathsf{Tr}_\alpha(P_0), \emptyset, id)$ is secure and there exists ta such that $\mathsf{ev}(d, ta, \mathsf{X}_\mathcal{E}\Sigma\sigma_1, \mathsf{F}\Sigma\sigma_1) \in tr_1$ with all agents in ta are honest. Hence, applying Definition 44 allows us to conclude.

Rule In: In such a case, $Q_1 = Q \mid \mathsf{in}_A(c, v).R_A$, $\Phi_2 = \Phi_1$, $\mu_2 = \mu_1$ and there exists σ such that $dom(\sigma) = vars(v\sigma_1)$ and either $v\sigma_1\sigma \in c\mu_1$ or else $c \in Ch_p \cup Ch_c$ and $\Phi_1 \vdash v\sigma_1\sigma$. Moreover, we have $P_2 = Q\sigma_1 \mid R_A\sigma_1\sigma$ and $\sigma_2 = \sigma_1\sigma$. Let us first define $Q_2 = Q \mid R_A$. In such a case, we deduce $Q_2\sigma_2 = P_2$.

Let us now define $\delta_2 = \delta_1 \cup \delta'$ where δ' is an injective mapping from tag_A-terms that are in σ but not in σ_1 or Φ_1 to fresh names of $\mathcal{N}_D$. In such a case, we directly have that δ_2 is a tag_A-mapping

of Φ_2 and σ_2. Moreover, let us define $tr_2 = tr_1$, $\mathsf{D}_2 = \mathsf{D}_1$, $\mathsf{N}_2 = \mathsf{N}_1$, $\mathsf{H}_2 = \mathsf{H}_1$, $\alpha_2 = \alpha_1$, $\beta_2 = \beta_1$, $\eta_2 = \eta_1$. We directly have that Φ_2 is a well formed frame for $\mathcal{S}$, D_2, N_2 and H_2. Since $\sigma_2 = \sigma_1\sigma$, then following Definition 49,we deduce that $Q_2, \Phi_2, \alpha_2, \beta_2, tr_2$ and σ_2 have conforming events. Moreover we also derive that $\eta_2\sigma_2 = \eta_1\sigma_1\sigma = \mu_1\sigma = \mu_1 = \mu_2$.

We now show that σ_2 is an executed substitution for Φ_2. We know that either $v\sigma_2 \in c\eta_1\sigma_1$ or else $\Phi_1 \vdash v\sigma_2$. In the former case, since η_1 only contains fully tag_B-terms, we deduce that all tag_A-tagged subterms of $v\sigma_2$ is a subterm of σ_1 and so the result holds since σ_1 is an executed substitution for $\Phi_1 = \Phi_2$. In the latter case, $\Phi_1 \vdash v\sigma_2$ and Lemma 30 directly allow us to conclude.

Since Q is an initial process, by Definition 47, we deduce that either v is a fully tag_B-tagged term and $c \notin img(\alpha_1) \cup img(\delta_1)$ or $v = \mathcal{E}\Sigma$ and $c = c_{pub} \in Ch_p$ where Σ is a fully tag_B-tagged substitution and $(\mathcal{E}, \mathsf{F})$ is an encapsulation. To prove the last property, we do a case analysis:

Case v is a tag_B-tagged term and $c \notin img(\alpha_1) \cup img(\delta_1)$: Since $Q_1 = Q \mid \mathsf{in}_A(c, v).R_A$ and $\alpha_1 = \alpha_2$, we deduce that $\mathsf{Tr}_{\alpha_1}(Q_1) = \mathsf{Tr}_{\alpha_2}(Q) \mid \mathsf{in}_A(c, v).\mathsf{Tr}_{\alpha_2}(R_A)$. But if $v\sigma_2 \in c\eta_1\sigma_1$ then $\mathsf{Ap}_{\delta_1}(v\sigma_1\sigma) \in \mathsf{Ap}_{\delta_1}(c\eta_1\sigma_1)$. But v and η_1 only containing fully tag_B-terms implies that $\mathsf{Ap}_{\delta_1}(v\sigma_1\sigma) = v\mathsf{Ap}_{\delta_1}(\sigma_1)\mathsf{Ap}_{\delta_1}(\sigma)$ and $\mathsf{Ap}_{\delta_1}(c\eta_1\sigma_1) = c\eta_1\mathsf{Ap}_{\delta_1}(\sigma_1)$. By definition of δ_2, we have that $\mathsf{Ap}_{\delta_1}(\sigma) = \mathsf{Ap}_{\delta_2}(\sigma)$ and so by considering the substitution $\mathsf{Ap}_{\delta_2}(\sigma)$, we deduce that:

$$(\mathsf{Tr}_{\alpha_1}(Q_1)\mathsf{Ap}_{\delta_1}(\sigma_1), \mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1), \eta_1\mathsf{Ap}_{\delta_1}(\sigma_1) \circ \mu(\Phi_1, \beta_1))$$
$$\rightarrow$$
$$(\mathsf{Tr}_{\alpha_2}(Q_2)\mathsf{Ap}_{\delta_2}(\sigma_2), \mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2), \eta_1\mathsf{Ap}_{\delta_1}(\sigma_1) \circ \mu(\Phi_2, \beta_2))$$

The mapping $\eta_1\mathsf{Ap}_{\delta_1}(\sigma_1)$ being ground, we have $\eta_1\mathsf{Ap}_{\delta_1}(\sigma_1) = \eta_1\mathsf{Ap}_{\delta_1}(\sigma_1) = \eta_1\mathsf{Ap}_{\delta_2}(\sigma_1)\mathsf{Ap}_{\delta_2}(\sigma) = \eta_2\mathsf{Ap}_{\delta_2}(\sigma_2)$. This allows us to conclude.

Let us now consider the case where $\Phi_1 \vdash v\sigma_2$. We know that $\delta_2 = \delta_1\delta'$, $\Phi_1 = \Phi_2$, $\mathsf{D}_2 = \mathsf{D}_1$, $\mathsf{N}_2 = \mathsf{N}_2$ and $\mathsf{H}_2 = \mathsf{H}_1$. Hence $\mathsf{Tr}^{\mathsf{H}_1,\delta_1}_{\mathsf{D}_1\cup\mathsf{N}_1,\emptyset}(\Phi_1) = \mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2)$. By Lemma 41, we deduce that $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash \mathsf{Ap}_{\delta_2}(v\sigma_2)$. Once again since v is a fully tag_B-tagged term, we deduce that $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash v\mathsf{Ap}_{\delta_2}(\sigma_2)$. Therefore, by considering the substitution $\mathsf{Ap}_{\delta_2}(\sigma)$, the result holds.

Case $v = \mathcal{E}\Sigma$ and $c = c_{pub} \in Ch_p$: In this case, by Definition 49, we deduce that there exists a channel d such that $((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha_1 = d$. Thus, we deduce that $\mathsf{Tr}_{\alpha_1}(Q_1) = \mathsf{Tr}_{\alpha_2}(Q_2) \mid \mathsf{in}_A(d, \mathsf{t}_{\mathcal{E}}\Sigma).\mathsf{Tr}_{\alpha_2}(R_A)$. Moreover, since $c \in Ch_p$, we deduce that $c \notin dom(\mu_1)$ and $\Phi_1 \vdash v\sigma_1\sigma$. To conclude the result, we show that

- if $d \in Ch_p$ then $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash \mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$
- if $d \in Ch_c$ then $\mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2) \in d\mu(\Phi_2, \beta_2)$ or $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash \mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$
- if $d \in Ch_a \cup Ch_s$ then $\mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2) \in d\mu(\Phi_2, \beta_2)$.

But using the same reasoning as in the case of the rule Out with $(\mathsf{Tr}_{\alpha_0}(P_0), \emptyset, id)$ being secure and the execution $(P_0, \emptyset, id) \overset{tr}{\Rightarrow}_\sigma (P, \Phi, \mu)$ being well-formed, we can deduce that if $d \in Ch_p$ then for all $k \in \mathsf{H}$, $\mathsf{X}_{\mathcal{E}_k}\mathsf{Ap}_{\delta_2}(\Sigma_k) \cap \mathsf{X}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2) = \emptyset$. However, if $d \in Ch_c \cup Ch_a \cup Ch_s$ then there exists $k \in \mathsf{H}$ such that $\mathsf{X}_{\mathcal{E}_k}\mathsf{Ap}_{\delta_2}(\Sigma_k) = \mathsf{X}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$. Moreover, we also know that $d \in Ch_c$ (resp. $Ch_a \cup Ch_s$) implies that $(\mathcal{E}, \mathsf{F})$ allows (resp. does not allow) confidential channels. Thus, by applying Lemma 43, we deduce that:

- if $d \in Ch_p$ then $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash \mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$.
- if $d \in Ch_c$ then either there exists $k \in \mathsf{H}$ such that $\mathcal{E}_k \sim \mathcal{E}$ and $\mathcal{E}_k\mathsf{Ap}_{\delta_2}(\Sigma_k) = \mathcal{E}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$ or $\mathsf{Tr}^{\mathsf{H}_2,\delta_2}_{\mathsf{D}_2\cup\mathsf{N}_2,\emptyset}(\Phi_2) \vdash \mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$. In the former case, by Definition 50, it implies that $\mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2) \in d\mu(\Phi_2, \beta_2)$ hence the result holds.
- if $d \in Ch_a \cup Ch_s$ then there exists $k \in \mathsf{H}$ such that $\mathcal{E}_k \sim \mathcal{E}$ and $\mathcal{E}_k\mathsf{Ap}_{\delta_2}(\Sigma_k) = \mathcal{E}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2)$ and so as previously, it implies that $\mathsf{t}_{\mathcal{E}}\Sigma\mathsf{Ap}_{\delta_2}(\sigma_2) \in d\mu(\Phi_2, \beta_2)$.

Rule New-k: In such a case, $Q_1 = Q \mid \mathsf{new}\ x.R_A$, $\Phi_2 = \Phi_1$, $\mu_2 = \mu_1$ and $P_2 = Q\sigma_1 \mid R_A\sigma_1\{^k/_x\}$ where k is a fresh name in $\mathcal{N}_H$ if $A \in \mathcal{A}gt_H$ else $k \in \mathcal{N}_D$. Therefore, the result trivially holds with $Q_2 = Q \mid R_A\{^k/_x\}$, $\Phi_2 = \Phi_1$, $\delta_2 = \delta_1$, $\eta_2 = \eta_1$, $\mathsf{D}_2 = \mathsf{D}_1$, $\mathsf{N}_2 = \mathsf{N}_1$, $\mathsf{H}_2 = \mathsf{H}_1$, $\beta_2 = \beta_1$ and $\alpha_2 = \{((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma\{^k/_x\}) \to c \mid ((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha_1 = c\}$.

Rule New-c: In such a case, $Q_1 = Q \mid \mathsf{new}\ c.Q'$, $\Phi_2 = \Phi_1$, $\mu_2 = \mu_1$ and $P_2 = Q\sigma_1 \mid R_A\sigma_1\{^{c'}/_c\}$ where c' is name in Ch_a (resp. Ch_c, Ch_s) if $c \in Ch_a$ (resp. Ch_c, Ch_s) and for all $I \in \mathcal{A}gt_D$, $c \in ch_I(Q')$ else $c' \in Ch_p$. Therefore, the result trivially holds with $Q_2 = Q \mid R_A\{^{c'}/_c\}$, $\Phi_2 = \Phi_1$, $\delta_2 = \delta_1$, $\eta_2 = \eta_1$, $\mathsf{D}_2 = \mathsf{D}_1$, $\mathsf{N}_2 = \mathsf{N}_1$, $\mathsf{H}_2 = \mathsf{H}_1$, $\beta_2 = \beta_1$ and $\alpha_2 = \alpha_1\{^{c'}/_c\}$.

Rule Repl: In such a case, $Q_1 = Q \mid !Q'$ where $dom(\sigma_1) \cap vars(Q') = \emptyset$, $\Phi_2 = \Phi_1$, $\mu_2 = \mu_1$ and $P_2 = Q\sigma_1 \mid !Q' \mid Q\rho$ where ρ is a fresh renaming of variables in Q'. We also know that the variables in Q_1 are bound once. Therefore, the result trivially holds with $Q_2 = Q \mid !Q' \mid Q\rho$, $\Phi_2 = \Phi_1$, $\delta_2 = \delta_1$, $\eta_2 = \eta_1$, $\mathsf{D}_2 = \mathsf{D}_1$, $\mathsf{N}_2 = \mathsf{N}_1$, $\mathsf{H}_2 = \mathsf{H}_1$, $\beta_2 = \beta_1$ and $\alpha_2 = \alpha_1 \circ \{((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma\rho) \to c \mid ((\mathcal{E}, \mathsf{F}), \mathsf{X}_{\mathcal{E}}\Sigma)\alpha_1 = c$ and $vars(img(\Sigma)) \cap dom(\rho) \neq \emptyset\}$.

Other rules: Trivial. ◂

Let S be a set of channels. We say that two process P and Q are *composable under S and C'* if $P = C[R_1, \ldots, R_n]$, $Q = C'[R'_1, \ldots, R'_n]$ and $C[\_] = C'[\_]|_{\overline{S}}$ for some contexts $C[\_], C'[\_]$ and for some roles R_i, R'_i of the same agent, for $i = 1 \ldots n$.

▸ **Theorem 17.** *Let tag_A and tag_B be two disjoint sets of tags. Let $\mathcal{S}_e$ be a set of tag_A-encapsulation allowing authentic, confidential, and secure channels. Let ρ be a mapping from channels to $T_{\mathcal{A}gt} \times \mathcal{S}_e$. Let P and Q be two closed executable composable tag_B-processes under ρ such that P and Q do not share names and $fa(P) = fa(Q) = \emptyset$. Let $\tilde{P}$ be an annotation of P under ρ. If $\tilde{P}$ is secure and Q preserves secrecy then $\tilde{P} \cdot^{\rho} Q$ preserves secrecy as well.*

Proof. Since P and Q are composable under ρ, let us denote $P = C[R_1, \ldots, R_n]$ and $Q = C'[R'_1, \ldots, R'_n]$. Moreover, following Definition 13, let us denote $\tilde{P} \cdot^{\rho} Q = C_0[R_1.R''_1, \ldots, R_n.R''_n]$ where $C_0 = \mathsf{C}^{C,C'|_{\overline{S}}}$ and $R''_1, \ldots, R''_n$ are defined as described in Definition 13 with $\tilde{P} = C[R_1.\mathsf{ev}_1(c_1, ta_1, ts_1, tp_1), \ldots, \tilde{R}_n.\mathsf{ev}_n(c_n, ta_n, ts_n, tp_n)]$.

Let us consider $\tilde{C}, C_1$ two contexts such that $\tilde{C}$ and C' are composable; and $\tilde{C}|_{\overline{S}} = C$. Let us denote $C_1 = \mathsf{C}^{\tilde{C},C'}$. Note that $C_0 = C_1|_{\overline{S}}$. Lastly, let us define γ a bijective mapping from S to fresh channels of same kind, that is $c\theta \in Ch_a$ (resp. Ch_c, Ch_s) is equivalent to $c \in Ch_a$ (resp. Ch_c, Ch_s).

We denote by $P_0 = C_1[\tilde{R}_1.R''_1, \ldots, \tilde{R}_n.R''_n]$. We first show that for all execution $(\tilde{P} \cdot^{\rho} Q, \emptyset, \emptyset, \emptyset) \overset{tr}{\Rightarrow} (P', \Phi, \mu)\theta$ there exists P'' and tr' such that $(P_0, \emptyset, \emptyset, \emptyset) \overset{tr'}{\Longrightarrow} (P'', \Phi, \mu)\theta$ is a well-formed execution and tr is the trace tr' where we removed the events of the form $ev(c, ta, ts, tp, d)$ with $ev \in \tilde{\mathsf{Ev}}$.

By construction, the differences between P_0 and $\tilde{P} \cdot^{\rho} Q$ lie the addition of some channel declarations in C_0 and the some events. But the declared channels are not used in any output or input of R_i and R''_i. Thus, we trivially have that for all execution $(\tilde{P} \cdot^{\rho} Q, \emptyset, \emptyset, \emptyset) \overset{tr}{\Rightarrow} (P', \Phi, \mu)theta$ there exists P'' and tr' such that $(P_0, \emptyset, \emptyset, \theta) \overset{tr'}{\Rightarrow} (P'', \Phi, \mu, \theta)$ and tr is the trace tr' where we removed the events of the form $ev(c, ta, ts, tp, d)$ with $ev \in \tilde{\mathsf{Ev}}$. The existence of a well-formed execution is then given by Lemma 46.

We now show that P_0 is an initial process and that there exists α_0 a mapping of channels for P_0 such that $\mathsf{Tr}_{\alpha_0}(P_0) = C_1[\tilde{R}_1.R'_1, \ldots, \tilde{R}_n.R'_n]$. We already know that P and Q are fully tag_B-tagged processes. Moreover, by Definition 13, we know that for all $i \in \{1, \ldots, n\}$, R''_i is the process R'_i where some instances of $\mathsf{out}_A(c, u)$ (resp. $\mathsf{in}_A(c, u)$) are replaced by $\mathsf{out}_A(c_{pub}, \mathcal{E}\sigma)$ (resp. $\mathsf{in}_A(c_{pub}, \mathcal{E}\sigma)$) when $c\rho = (ta, (\mathcal{E}, \mathsf{F}))$ and $\mathsf{event}_A(\tilde{\mathsf{ev}}_i(d, ta, \mathsf{X}_{\mathcal{E}}\sigma, \mathsf{F}\sigma, c))$ is in $\tilde{R}_i$ for some substitution σ. By Definition 47, we deduce that P_0 is initial.

Moreover, let us define α_0 such mapping such that for all $i \in \{1,\dots,n\}$, for all instances of $\mathsf{out}_A(c,u)$ (resp. $\mathsf{in}_A(c,u)$) in R'_i, if $\mathsf{event}_A(\mathsf{ev}_i(d,ta,\mathsf{X}_{\mathcal{E}}\sigma,\mathsf{F}\sigma,c))$ is in $\tilde{R}_i$ and $c\rho = (ta,(\mathcal{E},\mathsf{F}))$ for some $ta, c, (\mathcal{E},\mathsf{F})$ then $((\mathcal{E},\mathsf{F}),\mathsf{X}_{\mathcal{E}}\sigma)\alpha_0 = c$. Since by Definition 9, $c\rho = (ta,(\mathcal{E},\mathsf{F}))$ implies that $c \in Ch_a$ (resp. Ch_c,Ch_s) is equivalent to $(\mathcal{E},\mathsf{F})$ allows authentic (resp. confidential, secure) channels. Therefore, we can deduce from Definition 48 that α_0 is a mapping of channels for P_0. Lastly, following Definition 48 and Definition 13, we directly obtain that $\mathsf{Tr}_{\alpha_0}(P_0) = C_1[\tilde{R}_1.R'_1,\dots,\tilde{R}_n.R'_n]$.

Let us now prove that $(\mathsf{Tr}_{\alpha_0}(P_0),\emptyset,\emptyset,\emptyset)$ is secure. We know that $\tilde{P}$ is secure. But the properties of Definition 16 are all reachability properties which are preserved by parallel composition. Hence, we have that $(\tilde{P} \mid Q,\emptyset,\emptyset,\emptyset) = (C[\tilde{R}_1,\dots,\tilde{R}_n] \mid C'[R'_1,\dots,R'_n],\emptyset,\emptyset,\emptyset)$ is secure. But we know that P and Q do not share any names and $channels(C_1) \cap channels(R_1,\dots,R_n) \cap channels(R'_1,\dots,R'_n) = \emptyset$. Thus, a simple induction allows us to prove that $(C_1[\tilde{R}_1.R'_1,\dots,\tilde{R}_n.R'_n],\emptyset,id,=)(\mathsf{Tr}_{\alpha_0}(P_0),\emptyset,\emptyset)\emptyset$ is secure.

With the same reasoning as above, we can prove that $(C_1[\tilde{R}_1.R'_1,\dots,\tilde{R}_n.R'_n],\emptyset,\emptyset,\emptyset) = (\mathsf{Tr}_{\alpha_0}(P_0),\emptyset,\emptyset,\emptyset)$ preserves the secrecy of some term t shared by some agents $A_1,\dots,A_n$. We now show that $(P_0,\emptyset,id)$ also preserves the secrecy of t shared by $A_1,\dots,A_n$.

Let $(P_0,\emptyset,\emptyset,\emptyset) \overset{tr}{\Rightarrow}_\sigma (P',\Phi,\mu)\theta$ a well formed execution, and agent B and an event $\mathsf{Sec}(t',(A'_1,\dots,A'_n))$ such that $(B,\mathsf{Sec}(t',(A'_1,\dots,A'_n))) \in tr$ and $\Phi \vdash t'$. By Lemma 51, we deduce that there exists an initial process U, a mapping of channels α (resp. β) for U (resp. Φ), and η, δ, D, N and H such that:

- $U\sigma = P$; and
- $\eta\sigma = \mu$ and η only contains fully tag_B-terms; and
- U, Φ, α, β, tr and σ have conforming events; and
- Φ is a well formed frame for $\mathcal{S}_e$, D, N and H; and
- σ is an executed substitution for Φ; and
- δ is a tag_A-mapping of Φ and σ; and
- $(\mathsf{Tr}_\alpha(P_0),\emptyset,\emptyset,\emptyset) \overset{\mathsf{Ap}_\delta(tr)}{\Longrightarrow}_{\mathsf{Ap}_\delta(\sigma)} (\mathsf{Tr}_\alpha(U)\mathsf{Ap}_\delta(\sigma), \mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi), \eta\mathsf{Ap}_\delta(\sigma)\circ\mu(\Phi,\beta),\theta)$

But $(B,\mathsf{Sec}(t',(A'_1,\dots,A'_n))) \in tr$ implies that $(B,\mathsf{Sec}(\mathsf{Ap}_\delta(t'),(A'_1,\dots,A'_n))) \in \mathsf{Ap}_\delta(tr)$. Moreover, by Lemma 41 and Definition 36, $\Phi \vdash t'$ implies that $\mathsf{Tr}^{\mathsf{H},\delta}_{\mathsf{D}\cup\mathsf{N},\emptyset}(\Phi) \vdash \mathsf{Ap}_\delta(t')$. This is a contradiction with the fact that $(\mathsf{Tr}_{\alpha_0}(P_0),\emptyset,\emptyset,\emptyset)$ also preserves the secrecy of t shared by $A_1,\dots,A_n$. Therefore, $(P_0,\emptyset,\emptyset,\emptyset)$ indeed preserves the secrecy of t shared by $A_1,\dots,A_n$.

Note that in P_0 the channels $channels(C_1) \setminus channels(C)$ do not appear in any $\tilde{R}_i.R''_i$, for $i = 1..n$. As such, removing them still preserves the secrecy of t shared by $A_1,\dots,A_n$. Lastly, for all $i \in \{1,\dots,n\}$, the difference between $\tilde{R}_i$ and R_i is the addition of some event ev that are different from the event Sec, removing them also preserves secrecy meaning that $C[R_1.R''_1,\dots,R_n.R''_n] = \tilde{P} \overset{\rho}{,} Q$ preserves the secrecy of t shared by $A_1,\dots,A_n$. This allows us to conclude. ◂